HOUSE OF LORDS

European Union Committee

15th Report of Session 2007–08

The Passenger Name Record (PNR) Framework Decision

Report with Evidence

Ordered to be printed 3 June 2008 and published 11 June 2008

Published by the Authority of the House of Lords

London : The Stationery Office Limited
£price

HL Paper 106

The European Union Committee

The European Union Committee is appointed by the House of Lords "to consider European Union documents and other matters relating to the European Union". The Committee has seven Sub-Committees which are:
Economic and Financial Affairs and International Trade (Sub-Committee A)
Internal Market (Sub-Committee B)
Foreign Affairs, Defence and Development Policy (Sub-Committee C)
Environment and Agriculture (Sub-Committee D)
Law and Institutions (Sub-Committee E)
Home Affairs (Sub-Committee F)
Social and Consumer Affairs (Sub-Committee G)

Our Membership

The Members of the European Union Committee are:

Lord Blackwell
Baroness Cohen of Pimlico
Lord Dykes
Lord Freeman
Lord Grenfell (Chairman)
Lord Harrison
Baroness Howarth of Breckland
Lord Jopling
Lord Kerr of Kinlochard
Lord Maclennan of Rogart
Lord Mance
Lord Plumb
Lord Powell of Bayswater
Lord Roper
Lord Sewell
Baroness Symons of Vernham Dean
Lord Tomlinson
Lord Wade of Chorlton
Lord Wright of Richmond

The Members of the Sub-Committee which carried out this inquiry (Sub-Committee F) (Home Affairs) are:

Lord Dear
Baroness Garden of Frognal
Lord Harrison
Baroness Henig
Lord Hodgson of Astley Abbotts
Lord Jopling (Chairman)
Lord Marlesford
Lord Mawson
Lord Teverson
Lord Young of Norwood Green

Information about the Committee

The reports and evidence of the Committee are published by and available from The Stationery Office. For information freely available on the web, our homepage is:
http://www.parliament.uk/parliamentary_committees/lords_eu_select_committee.cfm
There you will find many of our publications, along with press notices, details of membership and forthcoming meetings, and other information about the ongoing work of the Committee and its Sub-Committees, each of which has its own homepage.

General Information

General information about the House of Lords and its Committees, including guidance to witnesses, details of current inquiries and forthcoming meetings is on the internet at
http://www.parliament.uk/about_lords/about_lords.cfm

Contacts for the European Union Committee

Contact details for individual Sub-Committees are given on the website.
General correspondence should be addressed to the Clerk of the European Union Committee, Committee Office, House of Lords, London, SW1A 0PW
The telephone number for general enquiries is 020 7219 5791.
The Committee's email address is euclords@parliament.uk

CONTENTS

	Paragraph	Page
Foreword—What this report is about		**5**
Chapter 1: Introduction		**7**
Passenger Name Record (PNR)	1	**7**
The EU/US PNR Agreement: our earlier inquiry	7	**8**
The draft Framework Decision	8	**8**
Striking the balance	10	**9**
This inquiry	12	**9**
Chapter 2: The draft Framework Decision		**11**
The draft Framework Decision in outline	15	**11**
The positive obligations	18	**11**
Data categories: PNR and API	22	**12**
Limitations and restrictions	25	**13**
Data protection	27	**13**
Review of operation	30	**14**
Chapter 3: Current Issues		**15**
The Government's strategy	31	**15**
The purpose limitation	38	**16**
The purpose limitation: conclusions and recommendations	50	**19**
The limitation to air transport, and the geographical scope	54	**20**
Chapter 4: Summary of Conclusions and Recommendations	66	**23**
Appendix 1: Sub-Committee F (Home Affairs)		**24**
Appendix 2: List of Witnesses		**25**
Appendix 3: PNR and API data categories		**26**
Appendix 4: List of Abbreviations		**28**
Appendix 5: Other Reports from the Select Committee		**29**

Oral Evidence

Ms Meg Hillier MP, Parliamentary Under Secretary of State,Mr Tom Dodd, Director of Border & Visa Policy, Border & Immigration Agency & Mr Kevan Norris, Legal Adviser, Home Office

Explanatory Memorandum, 20 November 2007	1
Written evidence, 18 March 2008	8
Oral evidence, 19 March 2008	10
Supplementary evidence, 7 April 2008	22
Further supplementary evidence, 4 May 2008	24

Ms Sophie in't Veld, MEP & Ms Linda van Renssen

Oral evidence, 2 April 2008	26

Ms Cecilia Verkleij, Head of Sector, & Ms Despina Vassiliadou, European Commission

Oral evidence, 2 April 2008	37

Mr Peter Hustinx, European Data Protection Supervisor, &
Mr Hielke Hijmans & Mrs A C Lacoste, Legal Advisers, EDPS Secretariat
Oral evidence, 2 April 2008 50

Written Evidence

Information Commissioner 59

Note: References in the text of the Report are as follows:
(Q) refers to a question in oral evidence
(p) refers to a page of written evidence

FOREWORD—What this report is about

In 2006 there were 200 million passenger movements across the United Kingdom's borders. By 2015 the annual figure is expected to have risen to 300 million. Basic information about those entering and leaving the country has been collected for many years, but more recently the threat of terrorism and other serious organised crime has made it important to collect and analyse fuller information—Passenger Name Record or PNR data—from which aspects of a passenger's history and conduct can be deduced, and further inquiries made if this seems necessary.

The United Kingdom and some other countries already collect PNR data. In the case of the United Kingdom this is done as part of the e-Borders project. Now there is an EU initiative which would require all Member States to collect PNR data and to share them with other Member States. Negotiations on the draft Framework Decision are at an early stage, but it is already clear that the United Kingdom and some other States believe that the draft does not go far enough; they would like to see PNR data collected and exchanged for purposes other than fighting terrorism and organised crime. They would also like the Framework Decision to cover forms of travel other than air travel between the EU and third countries.

In this short inquiry we have been looking at the position the Government are adopting in these negotiations. To some extent this has involved considering the draft Framework Decision itself. We have particularly been looking to see whether the draft, in its current form or as amended during negotiations, will be striking the right balance between the wide collection and use of data for security purposes and the rights of individuals to protection of their private and personal data

The Passenger Name Record (PNR) Framework Decision

CHAPTER 1: INTRODUCTION

Passenger Name Record (PNR)

1. Passenger Name Record data, or PNR data, are detailed data about passengers, mostly personal and confidential, which airlines have for many years collected for their own operational and commercial purposes, but which they are now increasingly obliged to communicate to the authorities of the country of destination. The prime purpose of this is the combating of terrorism and serious organised crime. At its most basic, this enables the authorities of the country of destination to follow the movements of those about whom they already have suspicions, and to identify from their details and habits other passengers about whom they ought perhaps to have suspicions. They can then, if they wish, prevent passengers from entering the country, or use the information to prevent the commission of serious offences or identify those who have committed them.

2. Many countries have been collecting the PNR data of incoming passengers for a number of years; those countries include the United States, Canada and Australia. Among the Member States of the EU, the United Kingdom is at present the only country to have a fully functioning PNR system. Under it information on individuals will be captured before they enter the United Kingdom, with the aim of authorising or denying them permission to set off for Britain. This is part of the electronic borders (e-Borders) programme, which is more fully described in supplementary evidence from the Home Office, as is Project Semaphore, the e-Borders pilot project (p 22).[1] We think it important to emphasise that, while by April 2009 e-Borders will be able to handle data for 100 million passenger movements a year, and for 95% of passengers in and out of the United Kingdom by the end of 2010, 100% coverage of all passenger movements across all United Kingdom borders will not be achieved until March 2014.

3. France and Denmark have legislation for a PNR system in place, and other Member States are showing an interest. Now the EU has its own initiative: a draft Framework Decision which, if adopted in anything like its current form, will enable the authorities of all the Member States to collect PNR data in respect of passengers on flights entering the EU from third countries, to analyse those data, and to share them with the authorities of other Member States.

4. We have sympathy with those who argue that collecting PNR data is no more than a sensible precaution which any State should take before letting anyone into the country. Commenting on the requirements now imposed by the United States, the President of the Centre for a New Europe thought that "the most basic security precautions surely involve cross-checking

---

1 There are also details of the e-Borders programme in *Securing the UK Border: Our vision and strategy for the future*, Home Office, March 2007.

passengers' data against suspicious behaviour patterns", and he added: "No one is compelled to hand over any information to the US, because no one is compelled to fly there … If you don't like America's terms of entry, don't go".[2]

5. At the other extreme, no doubt there are passengers who object to any private and personal details about themselves being communicated to third parties for any purpose. We suspect however that most passengers would not greatly object to their personal details being passed to the authorities of another country if they could be sure that this would in fact contribute to preventing terrorism or other serious crime; that the information would be used for no other purpose; that it would be transmitted and kept securely; and that it would be destroyed as soon as possible after their travel.

6. A point which tends to be forgotten is that, because carriers collect PNR data for their own commercial purposes, they apply to the collection and processing of those data the standards of care and accuracy needed for their own purposes, and not the higher standards which would (or should) be applied if the data were collected specifically for law enforcement purposes.[3] The value of a PNR system will depend, among other things, both on the accuracy of the data and on the quality of the technology used to process them.

The EU/US PNR Agreement: our earlier inquiry

7. A PNR agreement is an agreement under which the State of destination which is the recipient of PNR data gives undertakings in relation to this information. Because that State's prime concern is its own security rather than protecting the data of incoming passengers, such undertakings can fall short of what most passengers would wish. Last year we conducted an inquiry into a succession of PNR agreements which the United States concluded first with the EC and then with the EU. Our report following that inquiry contains in Chapter 2 an analysis of the categories of PNR data in those agreements contrasting it with the more basic information from the Advance Passenger Information (API) system; an explanation of data profiling and data mining; a consideration of the positive value of PNR; and a warning of what can happen if the wrong conclusions are drawn from PNR data. We do not propose to repeat these matters here, and refer the reader to that report.[4]

The draft Framework Decision

8. The European Council held in March 2004, when negotiations on the first EC/US PNR Agreement were in progress, invited the Commission to bring forward proposals for a common EU approach to the use of PNR for law enforcement purposes. This was repeated later that year in the Hague Programme, and again at the extraordinary Council meeting held on 13 July 2005 after the London bombings. On 6 November 2007 the Commission brought out its proposal for a Council Framework Decision on the use of the Passenger Name Record (PNR) for law enforcement purposes—the draft

---

2 Stephen Pollard, The Times, Monday 10 March 2008.

3 Ms Sophie in't Veld MEP, Q 110.

4 *The EU/US Passenger Name Record (PNR) Agreement* (21st Report, Session 2006–07, HL Paper 108)

PNR Framework Decision. On 7 December 2007 the Home Office supplied us with a full and clear Explanatory Memorandum giving the Government's views on this proposal. We print it with the evidence (p 1).

9. Framework Decisions under Title VI of the Treaty on European Union currently require consultation of the European Parliament and unanimity in the Council.[5] However none of our witnesses saw any prospect of negotiations on this Framework Decision being concluded by the end of 2008, and the position will then change. Assuming the ratification of the Treaty of Lisbon and its entry into force on 1 January 2009, co-decision with the European Parliament will then be needed. The Council will operate by qualified majority voting (QMV) rather than unanimity, but the United Kingdom will have the right not to opt in to the Framework Decision.

Striking the balance

10. In our earlier report we referred to the balance which has to be struck between the security of the public and the privacy of the individuals who make up the public. We said, and we repeat, that the collection and retention of data for security purposes must be no more invasive of individual privacy than is necessary to achieve the objective for which they are collected.[6]

11. The Government too believe there is a balance to be struck: "We believe it is vital, and possible, to achieve a result that strikes an appropriate balance between the right to privacy and the right to security and will work with Member States towards ensuring the data protection safeguards included in the proposal are appropriate."[7] However the Government wish to put more weight into the security side of the equation, as is clear from their part in the negotiations on the Data Protection Framework Decision to which we refer in the following chapter.

This inquiry

12. The focus of our brief inquiry has been the reasons why the Government wish to make radical changes to the draft Framework Decision, and whether such amendments can be justified. The inquiry was conducted by Sub-Committee F, whose members are set out in Appendix 1. They took evidence from Meg Hillier MP, the Parliamentary Under-Secretary of State at the Home Office responsible for the policy, and visited Brussels to take

---

5 Title IV of the Treaty establishing the European Community (TEC) deals with Visas, Asylum, Immigration and other policies related to free movement of persons. These are known as first pillar matters. Title VI of the Treaty on European Union (TEU) deals with Police and Judicial Cooperation in Criminal Matters, which include the proposal on the use of PNR for law enforcement which is the subject of our inquiry. These are third pillar matters.
Decisions in third pillar matters are reached by unanimity, and cannot therefore be binding on the United Kingdom without its agreement. The European Parliament is only consulted. However decisions in first pillar matters are reached by qualified majority voting (QMV), and by co-decision with the European Parliament. Under a Protocol to the Treaty of Amsterdam negotiated in 1997 the United Kingdom does not take part in first pillar measures unless within three months of a proposal for legislation it exercises its right to do so—i.e. it "opts in" to the proposal.
The distinction between the first and third pillars will disappear when the Treaty of Lisbon comes into force on 1 January 2009. At that stage the United Kingdom will have the right to opt in to proposals on all these matters; if it decides not to do so, the resulting measure will not be binding on it.

6 *The EU/US Passenger Name Record (PNR) Agreement* (21st Report, Session 2006–07, HL Paper 108), paragraph 5.

7 Explanatory Memorandum, paragraph 30.

evidence from the Commission, from Mr Peter Hustinx, the European Data Protection Supervisor,[8] and from Sophie in't Veld MEP, the rapporteur of the LIBE Committee of the European Parliament[9] which is examining this proposal. A full list of witnesses is in Appendix 2. To all of them we are most grateful.

13. It has not been possible to consider the Government's views and their strategy for the negotiations without looking at whether the draft Framework Decision itself strikes the right balance between public security and individual privacy, even though this has not been a specific purpose of our inquiry. Inevitably some of the evidence has been relevant more to the Framework Decision itself than to the Government's intentions. In particular, we have received interesting views on the provisions on the use of sensitive data, on data profiling and on data protection. We believe this evidence will be of value in any wider study of the Framework Decision which we or others may subsequently undertake.

14. We make this report to the House for information.

---

8 The European Data Protection Supervisor, or EDPS, is an independent supervisory authority of the EU whose task is to make sure that the right to protection of personal data is respected by the EU institutions and bodies. It does so by monitoring processing of personal data by the EU administration; advising on policies and legislation that affect privacy; and co-operating with similar authorities, including the Information Commissioner in the United Kingdom, to ensure consistent data protection. The EDPS formal Opinion of 20 December 2007 on the draft Framework Decision can be found on its website: www.edps.europa.eu.

9 The Committee on Civil Liberties, Justice and Home Affairs. The rapporteur is the member of the Committee appointed to explore the topic in depth, liaising with the other institutions and more widely, and to prepare for the Committee a report which, once adopted by the Committee and by the Parliament as a whole, will represent their views.

CHAPTER 2: THE DRAFT FRAMEWORK DECISION

The draft Framework Decision in outline

15. The purpose of a Framework Decision is to harmonise the laws of the Member States in third pillar matters. Its consequences are the same as those of Directives in the first pillar: the provisions are binding on the Member States as to the result to be achieved, but leave to the national authorities the choice of form and methods.[10] This explains the brevity of the draft under consideration: it takes only twelve substantive articles to outline the result to be achieved, and the limitations on the manner of achieving it.

16. The objective of the Framework Decision is set out in Article 1: it "provides for the making available by air carriers of PNR data of passengers of international flights to the competent authorities of the Member States, for the purpose of preventing and combating terrorist offences and organised crime, as well as the collection and retention of those data by these authorities and the exchange of those data between them".

17. The expression "the purpose of preventing and combating terrorist offences and organised crime" is known as the purpose limitation, because the data may be used for no other purpose. This is by far the most important and controversial of the issues currently under negotiation, and we consider at some length in the following chapter both the shortcomings of this limitation in the current draft, and the Government's proposals to weaken this limitation still further.

The positive obligations

18. To achieve its objective the Framework Decision imposes on the Member States a number of positive obligations. Article 3 requires each Member State to designate an authority, the Passenger Information Unit or PIU, to collect from air carriers or their intermediaries the PNR data relating to international flights; these are defined as flights originating in a third country and scheduled to enter the territory of at least one Member State, or to depart from the territory of at least one Member State with a final destination in a third country. Thus in its current form the Framework Decision does not apply to travel between or within Member States. A flight from Zurich to Heathrow would fall within this definition, but a flight from Frankfurt to Heathrow would not, and nor would a flight from Manchester to Heathrow.

19. The data collected by a PIU remain with that authority; they are not passed to a central database. The PIU is then required to analyse the data, to identify from them those individuals who need further examination, and to pass their PNR data to the authorities of that Member State which are responsible for preventing and combating terrorist offences and organised crime. The PNR data may then be used by those authorities for the following purposes:

    - to identify persons who are or may be involved in a terrorist or organised crime offence, as well as their associates;
    - to create and update risk indicators for the assessment of such persons;

[10] Compare TEU Article 34(2)(b) and TEC Article 249.

- to provide intelligence on travel patterns and other trends relating to terrorist offences and organised crime; and
- in criminal investigations and prosecutions of terrorist offences and organised crime.

20. Where the PIU of a Member State has identified an individual as needing further examination, it may pass that person's PNR data to the PIU of other Member States for transfer to the competent authorities designated by those States. Additionally, and subject to limitations, the PNR data may be passed to the law enforcement authorities of third countries.

21. Member States must ensure that air carriers make the PNR data which are collected and processed in their reservation systems available to the PIU of the State which the flight is entering, transiting or leaving, though the carriers may, and frequently do, employ intermediaries for this purpose. There must be sanctions, including financial penalties, available against carriers and intermediaries which transmit incomplete or erroneous data.

Data categories: PNR and API

22. The data collected may not include sensitive personal data revealing the racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership of the traveller, nor data concerning his or her health or sex life. Such data, if collected, must be deleted. But this still leaves available the 19 categories of data listed in the Annex to the Framework Decision. We set these out in Appendix 3 to this report. They are almost identical to the categories listed in the EU/US Agreement which we criticised in our earlier report as being unduly wide.[11] We have not taken further evidence on this point in the course of this short inquiry, but we see no reason to resile from our earlier view.

23. We also set out in that Appendix the categories of Advance Passenger Information (API) data, since there is sometimes confusion between the two. API data are (or will be) collected on all passenger movements, both in and out of the country, and allow them all to be traced. PNR data are collected on a selective basis from a far smaller proportion of passengers, but the data range much more widely and, as the Home Office explain in their supplementary evidence (p 22), are very useful in identifying potentially high risk individuals whose identities have *not* yet come to the attention of the authorities. By contrast, API data are particularly useful where an individual *has* already come to their attention. API data are taken from the travel document itself, so that spellings and dates are transcribed more accurately; it is therefore API data that the Home Office use to check against watch lists.

24. Over four years ago a Directive was adopted obliging air carriers to communicate API data to the authorities in the case of flights from third countries to Member States.[12] The deadline for implementation was 5 September 2006 but, as Ms Cecilia Verkleij told us on behalf of the

---

11 *The EU/US Passenger Name Record (PNR) Agreement* (21st Report, Session 2006–07, HL Paper 108), paragraphs 95 to 99. We refer there to the 34 data elements in the draft Agreement. The Agreement ultimately concluded the following month (OJ L204/18 of 4.8.2007) lists 19 data elements, but some of the 34 have simply been amalgamated; there is almost no difference in the substance.

12 Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L261/24 of 6 August 2004.

Commission, not all Member States have yet implemented the Directive, and most of the systems are not yet operational. It is therefore not yet possible to tell how the data are being used by Member States and how efficient and useful the data are for the purposes for which they are collected (QQ 134–135).

Limitations and restrictions

25. There are limitations on what Member States may do with the data they receive. Article 7 of the Framework Decision, entitled "Exchange of Information", provides that data may be passed to the PIU of another Member State "only in such cases and to the extent that such transmission is necessary in the prevention and fight against terrorist offences and organised crime". A similar restriction applies to transmission to the law enforcement authorities of third countries.

26. There is an obligation imposed on PIUs to keep PNR data in a database for five years; thereafter they must be kept in a separate database for a further eight years, but accessed only in exceptional circumstances in response to a specific threat or risk. After this the data must be deleted unless they are being used for an ongoing criminal investigation. This is generally interpreted as a limitation on the time for which the data may be kept. The limitations in the 2007 EU/US Agreement are seven and eight years. The previous (2006) EU/US Agreement allowed data to be routinely kept for only 3.5 years, and even that was thought by the Assistant European Data Protection Supervisor to be excessive; he saw "an enormous disproportion between the effectiveness of that long period of retention and the results of that retention".[13]

Data protection

27. Article 11 currently provides that the Data Protection Framework Decision (DPFD), which is to be adopted at the Justice and Home Affairs Council in June 2008, will apply to the processing of data under the PNR Framework Decision. This, at the time when the PNR Framework Decision was being drafted, would have added useful data protection measures, since the Commission at that stage hoped that the DPFD would apply to both domestic and cross-border data processing. But, as Ms Verkleij told us, "it turned out differently". The political agreement reached in the Council limited the scope of application of the DPFD to cross-border matters, so that the transfer of data from the carriers (or their intermediaries) to government agencies is not covered by any EU-wide data protection arrangement (Q 161).

28. Although Ms Verkleij did not say so, we are aware from our scrutiny of draft EU legislation that the Government have been prominent among those who have sought to reduce the effectiveness of the draft DPFD to the point where it is hard to see what it will in fact apply to. In particular, Recital 24a and Article 27b of the latest draft that we have seen[14] provide that the DPFD is to have no application at all in the case of data exchanges governed by the instruments constituting Europol and Eurojust, or under the Schengen Information System (SIS) or the Customs Information System (CIS), or

---

[13] *The EU/US Passenger Name Record (PNR) Agreement* (21st Report, Session 2006–07, HL Paper 108), Q 206.

[14] Document 16069/07.

under the Prüm Decision.[15] Despite (or perhaps because of) this the Government are content with this text, and hope to see it adopted as soon as possible.[16]

29. Some Member States have suggested including in the PNR Framework Decision not simply a reference to the DPFD, but specific data protection provisions so as to make sure that guarantees similar to the DPFD are also applied to domestic transfers of data within the PNR Framework Decision (QQ 112, 161). These, if adopted, would under Article 27b of the draft DPFD take precedence over it. The Government have told us that "during negotiations [they] will endeavour to ensure that the data protection safeguards applied are as robust as possible".[17] **We believe that adequate and effective rules on data protection should be contained in the PNR Framework Decision itself, and we urge the Government to support this view in the course of the negotiations.**

Review of operation

30. Finally, Article 17 requires the Commission to undertake a review of the operation of the Framework Decision within three years of its entry into force, and to report to the Council. The review is to pay special attention to, among other things, adherence to the data protection safeguards, the period of retention of data and the quality of the risk assessments. These are matters of great interest to us and, we are sure, to other national parliaments and to the European Parliament. We hope that the Commission's report will be made available to us and to them.

---

15 Draft Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. An earlier draft was the subject of our report *Prüm: an effective weapon against terrorism and crime?* (18th Report, Session 2006–07, HL Paper 90).

16 Explanatory Memorandum on the DPFD of 20 February 2008.

17 Explanatory Memorandum on the PNR Framework Decision, paragraph 44 (p 6).

CHAPTER 3: CURRENT ISSUES

The Government's strategy

31. The Home Office, in their written and their oral evidence, have made no secret of their strategy. The positive obligations of the Framework Decision are for the most part obligations which the Government have already willingly undertaken for the United Kingdom, and which they would be happy to see imposed on other Member States. The result would be that data collected for flights entering, leaving and transiting the EU as a whole, and not merely the United Kingdom, would be collected to help the EU as a whole, and not just the United Kingdom, in the fight against terrorism and organised crime.

32. On the other hand, the Government believe that the limitations and restrictions on the collection and use of PNR data which are contained in the current draft go too far, in particular in the following three respects:

- the draft restricts the use of PNR to terrorism and organised crime; the Government would like it to be used for any serious crime, organised or not, and also for immigration control purposes;
- the draft covers only air travel; the Government would like to extend it to other forms of travel, or at least to make sure that the draft does not prevent the United Kingdom from doing so;
- the draft covers only flights between a Member State and a third country; the Government would like to extend it to intra-EU flights and even domestic flights, or at least to make sure the draft does not prevent the United Kingdom from doing so.[18]

33. As appears from its proposal, the Commission believes that the positive obligations go hand in hand with the limitations and restrictions. It is likely that many, perhaps most, Member States will take the same view. The Government's hopes of eliminating or at least reducing the limitations may therefore not come to fruition.

34. Whatever limitations are ultimately contained in the Framework Decision, the Government have no intention of letting the United Kingdom's freedom of action be constrained by them. Nor do they see any danger of this. As we have said, currently the Framework Decision requires unanimity. Any restrictions which were unacceptable to the United Kingdom would be avoided simply by blocking the draft. This would not be possible after the end of the year, when under the Treaty of Lisbon the applicable procedure becomes co-decision and QMV. At that stage, to avoid constraints, the United Kingdom would have to decline to opt in to the Framework Decision. Mr Tom Dodd, the Director of Border and Visa Policy at the Border and Immigration Agency, put it this way: "Either way, we have a degree of lock on how it would apply to the UK" (Q 13).

35. If a Framework Decision was agreed after the end of this year and the United Kingdom decided not to opt in, the position would be as follows. Within the remaining Member States the Framework Decision would govern the PNR data which could be collected, the purposes for which they could be used,

[18] Explanatory Memorandum, paragraphs 33–35 (p 5).

and other limitations on their use; and those Member States would have the duty to give those data to the other Member States bound by the Framework Decision (and hence not the United Kingdom), and the right to receive such data from them. The United Kingdom, meanwhile, would remain free to collect such data as it wished from carriers in relation to incoming flights, and to use them for any purposes permitted under our law, subject only to such safeguards as our law provides (and in particular the Data Protection Act 1998). It would not be required to pass such data to other Member States. Conversely those States would be under no obligation to pass to the United Kingdom data derived from international flights entering their countries.

36. It would be unfortunate not to be part of the EU's own PNR initiative, and not routinely to receive PNR data from other Member States; but, at least in the view of the Government, less unfortunate than having unacceptable constraints on their own freedom of action.

37. We consider in turn the purpose limitation, the limitation to air travel and the geographical scope.

The purpose limitation

38. The purpose or purposes for which PNR data may be collected and used is the most controversial aspect of this proposal, and indeed of any proposal connected with PNR. The combating of terrorism is always given in national and international instruments on the use of PNR as their prime aim. Whether the purpose should go wider than this, and if so how much wider, is the issue on which we have received most evidence. It is, in the Commission's view, "an issue of huge importance" (Q 117). Mr Hustinx, the European Data Protection Supervisor (EDPS), told us that "the purpose specification is the key element in making a particular proposal legitimate under the human rights standards, but is also the pivotal element of any data protection arrangement if you want to make the safeguards appropriate" (Q 168).

39. The European Council's invitation to the Commission to bring forward this Framework Decision was made in a Declaration on Combating Terrorism. Unlike many of the expressions used in such instruments, "terrorism" does have a tolerably clear and uniform meaning throughout the EU, since one of the purposes of the Council Framework Decision of 13 June 2002 on combating terrorism[19] is to approximate the definition of terrorist offences in the Member States.[20]

40. As we have said, Article 1 of the PNR Framework Decision provides that PNR data can be made available to the authorities of Member States "for the purpose of preventing and combating terrorist offences and organised crime". Without the last three words, this would impose a limitation on the

---

19 Framework Decision 2002/475/JHA on combating terrorism, OJ L164/03 of 22 June 2002.

20 *Ibid.*, recital (6). Article 1 defines as a terrorist offence one of a list of serious acts defined as offences under national law "which, given their nature or context, may seriously damage a country or an international organisation where committed with the aim of seriously intimidating a population, or unduly compelling a Government or international organisation to perform or abstain from performing any act, or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation". At the Justice and Home Affairs Council on 18 April 2008 agreement was reached on an amending Framework Decision which will add the following crimes to the list: public provocation to commit a terrorist offence, recruitment for terrorism, and training for terrorism.

use of the data which could without much difficulty be uniformly applied across the EU. But the addition of "and organised crime" in our view renders the limitation highly unsatisfactory. Is "organised crime" necessarily serious crime? Is it necessarily transnational? The recitals to the EU/US PNR Agreements refer to "terrorism and related crimes, and other serious crimes that are transnational in nature, including organised crime". This at least makes it clear that, in that context, "organised crime" is both serious and transnational. The only indication that there is to be any common understanding of the meaning of the expression in the Framework Decision is the suggestion in the Impact Assessment[21] that a definition could be taken from another Framework Decision which has yet to be agreed.[22]

41. However the Government see "organised crime", however defined, not as too wide a limitation but as an unacceptably narrow purpose; they would like to be able to use PNR data for any serious crime, organised or not, and also for immigration control purposes.[23] Ms Verkleij told us that the Commission could not at present contemplate dealing in a third pillar instrument with purposes, such as immigration, which are first pillar matters. However the situation would have to be reviewed once the Treaty of Lisbon was in force and had done away with those two pillars. Even at that stage the Commission would have great difficulty in using PNR for immigration, revenue and customs purposes without any limitation. "We are not convinced that PNR data are really made for servicing those purposes, but we also have to bear in mind the issue of proportionality …" (Q 118).[24]

42. Nevertheless discussions in the Council show that a large majority of Member States to some extent share the views of the United Kingdom Government, and now favour extending the purpose limitation to cover serious crime instead of, or possibly in addition to, organised crime (QQ 124, 118). For a definition of "serious crime" Ms Verkleij thought guidance could be obtained from the list in Article 2(2) of the Framework Decision on the European Arrest Warrant.[25] That list includes "facilitation of unauthorised entry and residence", which in her view could cover immigration offences (though not immigration matters generally) (Q 118). We can see that this long list of crimes may well be of some assistance, but it does also illustrate

---

21 Document 14922/07 ADD 1, page 34

22 The Commission proposal for a Framework Decision on the Fight Against Organised Crime, COM(2005)6 final, does not suggest a definition of organised crime as such. However Article 1 would define a criminal organisation as "a structured association, established over a period of time, of more than two persons, acting in concert with a view to committing offences which are punishable by deprivation of liberty or a detention order of a maximum of at least four years or a more serious penalty in order to obtain, directly or indirectly, a financial or other material benefit". It would then be an offence to direct or participate in a criminal organisation.

23 France favours using PNR data in the fight against terrorism and illegal immigration, but not for other crimes.

24 Proportionality is the principle that action by the Community shall not go beyond what is necessary to achieve the objectives of the Treaty establishing the European Community: TEC Article 5, and Protocol No 30.

25 Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) [2002] OJ L 190/1. The Select Committee reported twice during the negotiations on the Framework Decision: *Counter Terrorism: the European Arrest Warrant*, 6th Report, Session 2001–02, HL Paper 34, and *The European Arrest Warrant*, 16th Report, Session 2001–02, HL Paper 89, and has since reported again: *European Arrest Warrant—recent developments*, 30th Report, Session 2005–06, HL Paper 156.

the problem, since it includes crimes like murder and rape which, though undoubtedly serious, are seldom either organised or cross-border.

43. While the United Kingdom is therefore not alone in wishing to see a wider purpose limitation, it is uncertain whether many would wish to see PNR data used for the full range of purposes advocated by the Government. Ms Hillier's letter of 20 November 2007 to Commission Vice-President Frattini illustrates this (p 7). She sets out to explain the success of the use of PNR by the Home Office pilot for the e-Borders scheme, Project Semaphore. The cases she lists include offences of drug-smuggling and other undoubtedly serious offences; but they also include "two tobacco smugglers". We question whether most people would regard tobacco smuggling as the sort of serious offence which PNR is designed to combat; it is not, on its own, among the "serious offences" to which a European Arrest Warrant applies.

44. Most significant of all, Ms Hillier's letter contains no reference to terrorism, and none of the examples she lists bears any relation to terrorism. Likewise, in oral evidence she was unable to give an example of the successful use of PNR in relation to a terrorist-related offence. She did assert that PNR "has absolutely been a tool in tackling terrorism", and explained the problems of sharing information about this in public (Q 28). However such a statement is unpersuasive when not accompanied by even a claim that PNR has succeeded in preventing, or assisting in the prevention of, a single terrorist attack, or bringing to justice the perpetrators of such an attack. Similarly, Mr Hustinx told us that when the US Secretary of Homeland Security was addressing the European Parliament "he was careful to annex a list of some 20 or so examples to his speech and it was all about drugs and people evading paying taxes and things like that, but there was very little in terms of precision on terrorism" (Q 170).

45. Ms Hillier represents the view that PNR data are but one in an arsenal of weapons which can be used to deal on a day-to-day basis with crimes, not all of which would be regarded as particularly serious, and with combating illegal immigration even when this is unrelated to a criminal offence (QQ 2, 10, 15). Ms Sophie in't Veld MEP put to us the opposite view: that the capture and use of PNR data by the authorities should be used wholly exceptionally, and only where it can be shown to have helped in combating terrorism or other organised crimes of similar gravity.

46. Ms in't Veld looks not just for assertions that PNR data have been of assistance in tackling terrorism, but for evidence of this. So far she has not found it; nor has Mr Hustinx, who described such evidence as there was as "scanty" and "anecdotal" (Q 167). As Ms in't Veld said: "If the people who are proposing this are so convinced that it is useful then I am sure they have all the supporting evidence … It is just that they have never produced it and every time you get the same argument, 'Oh, no, we cannot tell you that for security purposes' … All we have asked for, for example, is facts and figures which would not give away any operational details … all you get are horror stories by Mr Chertoff[26] which impress his audience, but, sorry, we are legislators. If I put my stamp of approval as a Member of Parliament on the law then I want to be absolutely sure that it has a solid justification, and we

[26] Mr Michael Chertoff, the United States Secretary for Homeland Security, and as such signatory of the EU/US PNR Agreement of 2007.

just never get any proper evidence" (QQ 96–97). Ms Verkleij saw no reason to exclude parliaments from this kind of debate (Q 155).

47. Ms in't Veld accepted, as we do, that PNR data have been shown to have helped in combating and resolving other crimes—though it was not clear that some at least of them could not have been resolved in the absence of PNR data. In recent high profile cases—the murder of Theo van Gogh, 9/11, the Madrid bombings—the necessary information was already available from other sources, and the failure lay in inadequate analysis of it or not making it available to the right people (Q 109). What was needed, and what was lacking, was evidence that PNR data were essential for their stated purpose, the fight against terrorism (Q 73). Citizens had the right to know the purposes for which their data could and could not be used (QQ 75–77).

48. In our earlier report we reluctantly concluded that, having received no evidence to the contrary, we should accept ministerial and other statements that PNR data constituted a valuable weapon in the fight against terrorism. We did however add that it was an important principle of democratic accountability that Parliament should be able to reach its own conclusions, and not rely on statements from the executive.[27]

49. Our scepticism about the value of PNR data in combating terrorism was made clear to the Minister. At a late stage we have received from her further material, including specific examples. We do not print this material with the evidence, but it has sufficed to persuade us of two things. The first is that PNR data on their own are seldom, if ever, likely to prevent terrorist attacks or, subsequently, to identify the perpetrators. But the second is that **PNR data, when used in conjunction with data from other sources, can significantly assist in the identification of terrorists, whether before a planned attack or after such an attack.**

The purpose limitation: conclusions and recommendations

50. From this evidence on the purpose limitation we draw the following conclusions, and we make the following recommendations.

51. **PNR data should be used for law enforcement purposes only in the fight against terrorism and in combating other serious crime. There can be no justification for agreeing legislation which does not set out clearly the purposes for which and the conditions under which the data may be used.**

52. **Blanket expressions such as "organised crime" or "serious crime" are inadequate. The offences for which PNR data can be used must be defined as clearly as is possible given the differing legal systems involved. If a definition of "serious crime" is possible for the European Arrest Warrant, appropriate definitions can be found for the Framework Decision.**

53. **The Government should be aware that, by attempting to extend the purposes beyond what is acceptable to other Member States and to the European Parliament, they may be forced to opt out of the Framework Decision. They may then find that, on balance, the ability to use PNR data to assist in the combating of more routine crime,**

---

[27] *The EU/US Passenger Name Record (PNR) Agreement* (21st Report, Session 2006–07, HL Paper 108), paragraphs 22–23.

including immigration, revenue and customs offences, is insufficient compensation for an inability to use data collected by other Member States. We hope that the Government will take account of our views in balancing the advantages and disadvantages of participation.

The limitation to air transport, and the geographical scope

54. As we have said, the draft Framework Decision applies only to passengers on international flights; it does not apply to flights between or within Member States, or to other modes of transport. When the Commission was formulating its proposal it consulted all the Member States on these and other matters. Of the six largest Member States, Germany shared the view of the United Kingdom that flights between Member States should be covered, France was doubtful, while Italy, Spain and Poland (and nearly all the smaller States) wanted the Framework Decision restricted to flights to and from third countries. Spain and France wanted, like the United Kingdom, to include both sea and rail transport, while Germany, Italy and nine smaller Member States wanted in due course to include sea transport but not rail. Poland and the remaining Member States which replied wanted the Framework Decision restricted to air travel.[28]

55. It is probably true that if terrorists and other criminals are aware that a PNR system is in force which may identify them on their travels, but that it applies only to certain modes of transport, they will avoid them if there is any alternative. Ms Verkleij, while agreeing, thought this betrayed a misunderstanding of the system. "That takes as a presumption that PNR solves everything, and that is simply not the case. PNR is an additional tool, additional to the API data, to the visa, to other information, the aim of which should be to fit them into a jigsaw puzzle which we then present as tools to law enforcement next to other instruments which should allow law enforcement to look at particular ways of people entering our countries … [Our proposal aims] to give law enforcement information which it does not have now for particular modes of transport in addition to already existing means" (Q 149).

56. Member States were not asked by the Commission whether they wanted the Framework Decision to apply to road travel. Although the Home Office Explanatory Memorandum refers to "all modes of transport",[29] Ms Hillier in her letter of 18 March 2008 refers to "data from maritime and rail carriers, as well as from airlines", but does not refer to road transport (p 8). We believe this is just as well. Not only is the PNR system dependent on data being routinely collected by the carrier, but as Ms Verkleij pointed out it is also dependent on the data being available some time in advance of travel to allow the authorities access to them (Q 143).

57. In the case of air travel, even if tickets are bought at the last possible moment the data are still available some time before the actual departure of the passenger. This will often also be true of maritime travel. Ms Verkleij told us that, although PNR data could most effectively be collected for air transport, it was arguable that in Southern Europe there was competition between certain maritime links and air routes. If Member States thought there was a

---

[28] Commission Impact Assessment, document 14922/07 ADD 1, Annex B. Finland, Ireland and Malta did not express any views.

[29] Paragraph 35, p 5.

real issue, the proposal would allow them to implement domestic measures on sea travel which would take care of their security concerns. However data collection in the maritime sector was at present pretty limited (QQ 140–142).

58. Logically, the same arguments apply to rail transport. However data currently collected from rail travel are even more limited, and where tickets are not bought in advance there is virtually no time to act on the data. Only five Member States are interested in the Framework Decision applying to rail travel. These arguments will be even more valid in the case of road transport.

59. **Although we have not received any conclusive evidence on the topic, it seems to us that PNR data could not effectively be collected for rail transport, and that in the case of road transport the data do not exist.**

60. Ms Hillier would however like to apply the Framework Decision to travel through the Channel tunnel and to Eurostar (Q 32). We would support this.

61. We are not aware that there is currently any serious discussion in the Council about extending the draft Framework Decision to either sea or rail travel. If it remains restricted to air travel, those Member States which wish to use PNR data from other modes of travel will remain free to do so.

62. In the United Kingdom, the Immigration, Asylum and Nationality Act 2006 allows the use of PNR data from air, sea and rail carriers. The limitations on the use of the data are contained in the Code of Practice on the management of information shared by the Border and Immigration Agency, HMRC and the Police. This Code of Practice has a degree of Parliamentary sanction: it has to be laid before Parliament in draft,[30] and comes into force only by virtue of an Order which is a statutory instrument subject to negative resolution. The Code of Practice is not part of our inquiry. We only observe that Parliament has in fact approved it.[31]

63. Fourteen of the 27 Member States would like to see the Framework Decision apply sooner or later to sea travel. Since one of the purposes of the Framework Decision is to make a single system available for the benefit of States, carriers and passengers, with a single set of safeguards, it seems to us that, **if and when negotiations are successfully concluded on a PNR Framework Decision applicable to air travel, work should then begin on extending it to sea travel.**

64. If, as is likely, the proposal remains for the present limited to flights to and from third countries, there will be no obligation on Member States, whether under the Framework Decision or otherwise, to collect PNR data in relation to flights between Member States. If the United Kingdom collects such data in relation to flights entering the United Kingdom it will be under no obligation to share the data with other States, though there would seem to be nothing to prevent it from doing so, subject to data protection rules. Similarly, if some other Member States collect such data, they could be shared with the United Kingdom, but this would be under informal arrangements.

65. It does not necessarily follow that Member States remain free to seek what PNR data they like for travel between and within Member States.

---

30 Section 37 of the Immigration, Asylum and Nationality Act 2006.

31 The Immigration, Asylum and Nationality Act 2006 (Data Sharing Code of Practice) Order 208, S.I. 2008/8, which brought the Code of Practice into force on 1 March 2008.

Mr Hustinx pointed out that issues of freedom of movement and proportionality might arise, and other issues within the Schengen States (Q 177). But it is probably true to say that in the case of air travel, where the data are already being collected so that no additional restrictions on freedom of movement are imposed, those Member States which wish to make use of the data for law enforcement purposes will be able to do so.

CHAPTER 4: SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

66. We are persuaded that PNR data, when used in conjunction with data from other sources, can significantly assist in the identification of terrorists, whether before a planned attack or after such an attack. (paragraph 49)

67. PNR data should be used for law enforcement purposes only in the fight against terrorism and in combating other serious crime. There can be no justification for agreeing legislation which does not set out clearly the purposes for which and the conditions under which the data may be used. (paragraph 51)

68. Blanket expressions such as "organised crime" or "serious crime" are inadequate. The offences for which PNR data can be used must be defined as clearly as is possible given the differing legal systems involved. If a definition of "serious crime" is possible for the European Arrest Warrant, appropriate definitions can be found for the Framework Decision. (paragraph 52)

69. The Government should be aware that, by attempting to extend the purposes beyond what is acceptable to other Member States and to the European Parliament, they may be forced to opt out of the Framework Decision. They may then find that, on balance, the ability to use PNR data to assist in the combating of more routine crime, including immigration, revenue and customs offences, is insufficient compensation for an inability to use data collected by other Member States. We hope that the Government will take account of our views in balancing the advantages and disadvantages of participation. (paragraph 53)

70. We believe that adequate and effective rules on data protection should be contained in the PNR Framework Decision itself, and we urge the Government to support this view in the course of the negotiations. (paragraph 29)

71. Although we have not received any conclusive evidence on the topic, it seems to us that PNR data could not effectively be collected for rail transport, and that in the case of road transport the data do not exist. (paragraph 59)

72. If and when negotiations are successfully concluded on a PNR Framework Decision applicable to air travel, work should then begin on extending it to sea travel. (paragraph 63)

73. We make this report to the House for information. (paragraph 14)

APPENDIX 1: SUB-COMMITTEE F (HOME AFFAIRS)

The members of the Sub-Committee which conducted this inquiry were:

Lord Dear
Baroness Garden of Frognal
Lord Harrison
Baroness Henig
Lord Hodgson of Astley Abbotts
Lord Jopling (Chairman)
Lord Marlesford
Lord Mawson
Lord Teverson
Lord Young of Norwood Green

Declarations of Interests:

A full list of Members' interests can be found in the Register of Lords Interests:
http://www.publications.parliament.uk/pa/ld/ldreg.htm

APPENDIX 2: LIST OF WITNESSES

The following witnesses gave evidence. Those marked ⋆ gave oral evidence

⋆ Home Office, Ms Meg Hillier, MP, Parliamentary Under Secretary of State

⋆ Home Office, Border and Immigration Agency

⋆ Ms Sophie in't Veld , MEP

⋆ European Commission

⋆ European Data Protection Supervisor (EDPS)

Information Commissioner

APPENDIX 3: PNR AND API DATA CATEGORIES

Categories of PNR data for the purposes of the draft Framework Decision

Data for all passengers

(1) PNR record locator

(2) Date of reservation/issue of ticket

(3) Date(s) of intended travel

(4) Name(s)

(5) Address and Contact information (telephone number, e-mail address)

(6) All forms of payment information, including billing address

(7) All travel itinerary for specific PNR

(8) Frequent flyer information

(9) Travel agency /Travel agent

(10) Travel status of passenger including confirmations, check-in status, no show or go show information

(11) Split/Divided PNR information

(12) General remarks (excluding sensitive information)

(13) Ticketing field information, including ticket number, date of ticket issuance and one way tickets, Automated Ticket Fare Quote fields

(14) Seat number and other seat information

(15) Code share information

(16) All baggage information

(17) Number and other names of travellers on PNR

(18) Any collected API information

(19) All historical changes to the PNR listed in numbers 1 to 18

Additional data for unaccompanied minors under 18 years

(1) Name and gender of child

(2) Age

(3) Language(s) spoken

(4) Name and contact details of guardian on departure and relationship to the child

(5) Name and contact details of guardian on arrival and relationship to the child

(6) Departure and arrival agent

Categories of API data for the purposes of Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data

(1) Number and type of travel document used

(2) Nationality

(3) Full names

(4) Date of birth

(5) Border crossing point of entry into the territory of the Member States

(6) Code of transport

(7) Departure and arrival time of the transportation

(8) Total number of passengers carried on that transport

(9) Initial point of embarkation

APPENDIX 4: LIST OF ABBREVIATIONS

API	Advance Passenger Information
Article 29 Working Party	Data Protection Working Party established under Article 29 of the Data Protection Directive 95/46/EC
BIA	Border and Immigration Agency
DHS	United States Department of Homeland Security
DG JLS	Directorate-General Justice Freedom and Security of the Commission
DPFD	Data Protection Framework Decision
EAW	European Arrest Warrant
EC	European Community
EDPS	European Data Protection Supervisor
EU	European Union
ICO	Information Commissioner's Office
JHA	Justice and Home Affairs
LIBE Committee	Committee on Civil Liberties, Justice and Home Affairs of the European Parliament
PIU	Passenger Information Unit set up under Article 3 of the draft Framework Decision
PNR	Passenger Name Record
QMV	Qualified majority voting
TEC	Treaty establishing the European Community
TEU	Treaty on European Union

APPENDIX 5: OTHER REPORTS FROM THE SELECT COMMITTEE

Recent Reports from the Select Committee

Annual Report 2007 (36th Report, Session 2006–07, HL Paper 181)

The Treaty of Lisbon: an impact assessment (10th Report, Session 2007–08, HL Paper 62)

Relevant Reports prepared by Sub-Committee F

Session 2004–05

After Madrid: the EU's response to terrorism (5th Report, HL Paper 53)

The Hague Programme: a five year agenda for EU justice and home affairs (10th Report, HL Paper 84)

Session 2005–06

Behind Closed Doors: the meeting of the G6 Interior Ministers at Heiligendamm (40th Report, HL Paper 221)

Session 2006–07

After Heiligendamm: doors ajar at Stratford-upon-Avon (5th Report, HL Paper 32)

Prüm: an effective weapon against terrorism and crime? (18th Report, HL Paper 90)

The EU/US Passenger Name Record (PNR) Agreement (21st Report, HL Paper 108)

Session 2007–08

FRONTEX: the EU external borders agency (9th Report, HL Paper 60)

Minutes of Evidence

TAKEN BEFORE THE EUROPEAN UNION COMMITTEE (SUB-COMMITTEE F)

WEDNESDAY 19 MARCH 2008

Present	Dear, L	Hodgson of Astley Abbotts, L
	Garden of Frognal, B	Jopling, L (Chairman)
	Harrison, L	Marlesford, L
	Henig, B	Mawson, L

Memoranda by the Home Office

Council Document: 14922/07

COM (2007) 654 final

EXPLANATORY MEMORANDUM (EM) ON EUROPEAN COMMUNITY LEGISLATION

European Commission proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes.

Submitted by the Home Office on 7 December 2007

SUBJECT MATTER

1. This EM relates to a Commission proposal for a Council Framework Decision on the use of PNR for law enforcement purposes. The proposal aims to harmonise Member States' provisions on obligations for air carriers operating flights between at least one Member State and a non-EU state regarding the transmission of PNR data to the competent authorities for the purpose of preventing and fighting terrorist offences and organised crime, It will provide for rules governing the subsequent use and retention of that data by these authorities and the exchange of that data between them. The proposal also envisages that all processing of PNR data under the proposal will be govemed by the Council Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters.

2. The Commission submitted this proposal to Mr Javier SOLANA, Secretary-General/High Representative on 12 November.

DEFINITIONS

3. *Passenger Name Record (PNR):* in the air transport industry, is the generic term for records created by aircraft operators or their authorised agents for each journey booked by or on behalf of any passenger. The data is used by airline operators for their own commercial and operational purposes in providing air transportation services. A PNR is built up from data supplied by or on behalf of the passenger concerning all the flight segments of a journey eg passenger's name, address, telephone numbers, ticketing field information, travel itinerary etc. This data may be added to by the operator or his authorised agent eg changes to requested seating, additional services etc.[1] Outside the airline industry, PNR data is also known as Other Passenger Information (OPI).

4. In this proposal, PNR is defined as "a record of each passenger's travel requirements which contains all information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person. In the context of this Framework Decision, PNR data shall mean the data elements described in the Annex and only to the extent that these are collected by the air carriers".

[1] Definition from International Civil Aviation Organization (ICAO) Guidelines paper on Passenger Name Record (PNR) Data 12/08/05. p 2.

5. *Advance Passenger Information (API):* is the main biographical data on an individual given to a state, prior to that individual's arrival in a country. This information usually consists of data found in the Machine Readable Zone (MRZ) of ICAO Document 9303 compliant travel documents. Key API data consists of full name of the traveller, date of birth, gender, nationality, travel document type, country of issue and travel document number.[2] As this is an airline term, API data is known as Travel Document Inforrnation (TDI) to other carriers.

6. The grounds and objectives of the proposal are based on the Commission's view, which we share, that terrorism constitutes a major threat to security, peace, stability, democracy and fundamental rights. The *EU Terrorism Situation and Trend Report 2007* of Europol identified that almost all terrorist campaigns are transnational, The internal and external aspects of the fight against terrorism are interlinked. For any measures to be effective, close cooperation and enhanced exchange of information between EU Member States and their respective services, as well as Europol and, where appropriate, the competent authorities of third countries, is necessary. These issues are equally pertinent for organised crime as the use of passenger data will greatly enhance our ability to gain intelligence on criminals and identify those who may pose a risk. Joint EU cooperation in this area will greatly strengthen the UK's ability to combat both terrorism and organised crime activities.

7. Until now, only a limited number of Member States have adopted legislation to set up mechanisms to oblige carriers to provide the relevant PNR data and to have such data analysed by the competent authorities. The Commission believes this may mean that the potential benefits of an EU wide scheme in preventing terrorism and organised crime are not fully realised.

8. The European Council on 25–26 March 2004 invited the Commission to bring forward a proposal for a common EU approach to the use of passengers' data for law enforcement purposes.

Existing Provisions

9. Currently carriers have an obligation to communicate some passenger data to the competent authorities of EU Member States, under Council Directive 2004/82/EC. The data included here is usually referred to as API data, however it also includes some elements of service data.[3] This Directive provides that, in order to combat illegal immigration effectively and to improve border control, it is essential that all Member States introduce provisions laying down obligations on air carriers transporting passengers into the territory of the Member States to communicate the required passenger data to the competent authorities. The obligation to provide this data to a MS under the Directive only relates to flights arriving into that MS from a non-EU State, however it also contains caveats allowing Member States to retain or introduce additional obligations for air carrier or some categories of other carriers, whether referred to in this Directive or not. In addition, it requires that sanctions, above a specified minimum or up to a specified maximum must be imposed for non-compliance. Council Directive 2004/82/EC applies to the UK.

10. Currently, an individual agreement relating to the transmission of certain PNR by air carriers in respect of flights between the EU and the US and an individual agreement relating to the transmission of certain PNR and API data by air carriers in respect of flights between the EC and Canada have been concluded. The agreements require air carriers that already capture passenger data on flights between the EU and the relevant country to transmit this data to the competent authorities of that country. On the basis of an exchange of information with these third countries, the EU has been able to assess the value of PNR data and to realise its potential for law enforcement purposes. The EU has also been able to learn from the experiences of such third countries in the use of PNR data, as well as from the experience of the UK's test of concept trial, Project Semaphore. An agreement between the EU and Australia on the transfer of PNR data from flights between the Member States and Australia is also expected to be negotiated shortly.

Consultation of Interested Parties

11. The Commission services consulted all Member States, the data protection authorities of all Member States, the European Data Protection Supervisor (EDPS), the Association of European Airlines (AEA), the Air Transport Association of America (ATAA), the International Air Carrier Association (IACA), the European Regions Airline Association (ERA) and the International Air Transport Association (IATA).

[2] Definition from International Civil Aviation Organization (ICAO) Guidelines paper on Passenger Name Record (PNR) Data 12/08/05 Annex 3 p 13, with the exception of "This information . . . documents", taken from the International Air Transport Association (IATA) website at: http://www.iata.org/whatwedo/safety_security/facilitation/index.htm (28 November 2007).

[3] The element of data requested are listed as: the number and type of travel document used, nationality, full names, date of birth, the border crossing point of entry into the territory of the Member States, code of transport, departure and arrival time of the transportation, total number of passengers carried on that transport and the initial point of embarkation.

12. Please see para 33 and 36 for details of the UK consultation and impact Assessment relating to the government's upcoming secondary legislation to capture passenger data.

Scrutiny History

13. None.

Ministerial Responsibility

14. Following cross-governmental consultation, it has been agreed that the Home Secretary will lead the negotiations on the proposal. This proposal is also of particular interest to the Secretary of State for Justice, the Secretary of State for Transport, the Foreign Secretary and the Financial Secretary to the Treasury.

Interest of the Devolved Administrations

15. Scottish police have access to PNR data for reserved purposes. We are consulting the Devolved administrations to consider the application of this proposal in more detail.

Legal and Procedural Lines

(i) *Legal basis*

16. The Treaty on European Union (TEU), and in particular Article 29, Article 30(1)(b) and Article 34(2)(b).

(ii) *European Parliament procedure*

17. Consultation.

(iii) *Voting procedure in the Council*

18. Unanimity.

(iv) *impact on UK law*

Existing Provisions

19. The UK currently has the ability to collect certain passenger, service and crew data under the powers of the Commissioners' Directions of the Customs and Excise Management Act 1979, paragraphs 27 and 27B of Schedule 2 to the Immigration Act 1971 and paragraph 17 of Schedule 7 to the Terrorism Act 2000. There are powers for this data to be shared on a case by case basis between the Border Agencies under section 19 of the Anti-Terrorism, Crime and Security Act 2001 and sections 20 and 21 of the Immigration and Asylum Act 1999.

20. The information that can be obtained under paragraphs 27 and 27B of Schedule 2 to the Immigration Act 1971 is to be extended (to cover service information and more PNR elements) by legislation to be introduced at the beginning of 2008. The police will also lay new powers to acquire API and PNR data at the same time (section 32 of the Immigration, Asylum and Nationality Act 2006 and secondary legislation under that provision). Therefore, from early 2008 there will be powers to obtain passenger, service and crew data on a routine basis from all air, rail and maritime carriers on routes entering or leaving the United Kingdom. The form and manner in which this data should be supplied will also be specified. Forthcoming secondary legislation under Channel Tunnel Act 1987 will apply and modify the various data acquisition powers to trains running between Belgium/France and the UK.

21. The Immigration, Asylum and Nationality Act 2006 (Duty to Share Information and Disclosure of information for Security Purposes) Order 2008, to be brought into force alongside the above powers, will specify the information which must be shared between the Border Agencies pursuant to section 36 of the Immigration, Asylum and Nationality Act 2006. That will also be applied to trains running between Belgium/France and the UK.

Legislation needed to Implement the Proposal

22. The current powers and forthcoming UK legislation as described above, will allow for the collection of the PNR data requested under the EU proposal. However as currently drafted the terms of the proposal may run counter to some of these provisions of UK law. Therefore, were the proposal to be adopted as currently drafted, UK legislation may need to be amended. These issues are set out later in the document.

(v) *Application to Gibraltar*

23. The Government of Gibraltar is being consulted on participation in this measure.

(vi) *Fundamental Rights Analysis (FRA)*

24. The Framework Decision provides for the acquisition, use and sharing of personal data and therefore engages Article 8 of the European Convention on Human Rights (right to respect for private and family life). However, any interference with Article 8 rights would be justified under Article 8(2) of the Convention because the Framework Decision:

(a) restricts the purposes for which data can be processed to purposes included within Article 8(2) (as currently drafted, these purposes are restricted in the proposal to the prevention of and fight against terrorist offences and organised crime);

(b) makes express provision for data security in article 11;

(c) provides that the Council Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters applies to the processing of personal data under the proposal; and

(d) only permits onward transmission to a third country in accordance with national law and on the condition that it will only be used for the purpose of preventing and fighting terrorist offences and organised crime and that it will not be further transmitted to another third country without the express consent of the Member State.

25. Accordingly, in the opinion of the Minister the agreement should be regarded as respecting fundamental rights.

Application to the European Economic Area

26. This document will not apply to Iceland, Liechtenstein or Norway.

Subsidiarity

27. The Commission believes that the objectives of this proposal cannot be achieved sufficiently by Member States acting alone. The Council may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty establishing the European Community (TEC) and referred to in Article 2 of the TEU. in accordance with the principle of proportionality, as set out in Article 5 of TEC, this proposed Framework Decision does not go beyond what is necessary to achieve those objectives.

28. The UK government is confident that this is a proper area for Europe-wide action. The legislation will set the overseas legal principles for use and exchange of PNR data not only in Europe but beyond. This will underpin our ability to collect PNR data for a wide-range of purposes and encourage the development of parallel EU systems and data exchange powers.

Policy Implications

29. The Government welcomes the Commission's proposal. Passenger information is central to a fundamentally more effective, efficient and secure border and greater cooperation in the EU will increase the benefits and effectiveness of our domestic programme. This proposal has the potential to be an important tool to share data in the fight against criminality targeting our borders.

30. Our view is that this should be a permissive framework which sets a basis for collection and sharing of PNR and enables our authorities to use this data to maintain the security and integrity of our borders. In particular we need to allow the processing and exchange of PNR data for wider border security and crime-fighting purposes such as immigration and customs purposes. We believe it is vital, and possible, to achieve a

result that strikes an appropriate balance between the right to privacy and the right to security and will work with Member States towards ensuring the data protection safeguards included in the proposal are appropriate.

31. The UK has already had great success in this area. The e-Borders pilot, Project Semaphore—has demonstrated how effective use of this additional data can be, with over 1,300 arrests to date. To further illustrate the benefits experienced by the UK in this area to our European counterparts, I have written to Commissioner Frattini, copied to my JHA colleagues as annexed.

32. This proposal as drafted will have implications for forthcoming UK secondary legislation (we intend to lay before Parliament in the New Year) relating to PNR data and subsequently the implementation of the UK's domestic passenger data programme—e-Borders. We will therefore work to ensure that the proposal is compatible with the UK programme and wider domestic powers.

There are a number of issues in the proposal:

Scope

33. As drafted, the proposal would only enable the use of PNR data to prevent or combat terrorist offences and organised crime (Article 3). Our initial assessment of the effect of the proposal is that there is a significant risk that it would constrain our ability to process this data for the purposes of combatting, for example, individual serious crime, We therefore will need to negotiate a wider scope.

34. PNR data has been shown to be a key tool under Semaphore, providing the mechanism to identify those who may pose a risk, spot emerging trends, track suspects in advance, and trace missing and other vulnerable subjects. Key successes to date through PNR data analysis and tracking include the offloading of passengers attempting to smuggle swallowed drugs to the UK, identification of a significant number of facilitators including those using falsified documents, and a number of serious crime suspects. Therefore, PNR data has been shown to be particularly valuable for purposes other than counter terrorism and organised crime.

35. The proposal would enable the collection of data from flights between the EU and a third country. Given that the risk to security is spread across all modes of transport we will seek to ensure, that like existing API legislation, this proposal does not restrict Member State's ability to collect and process data for other modes of transport, or to collect data on intra-EU journeys.

Competent Authorities

36. Linked to the issue on scope, the proposal enables authorities whose functions include the prevention or combating of terrorist offences and organised crime to be considered a Competent Authority, and thus authorised to be a Passenger Information Unit (PIU), permitted to process PNR (Article 11). We will seek to ensure that the proposal takes account of the wider range of agencies permitted to process this data in UK law can do so.

Exchange of Information

37. Under the proposal, PNR data is only to be provided to law enforcement authorities of countries outside the EU for the purpose of preventing and fighting terrorist offences and organised crime, and must not be transferred onwards to another third country without the express consent of the Member State providing the data. Any such exchange would be within the context of national law, applicable international agreements and the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Article 8). The UK would want to retain our current legal powers regarding the exchange of data, and therefore will need to ensure that any EU legislation enables this.

Timing

38. The proposal restricts carriers to providing PNR data 24 hours in advance of travel, preventing them from providing data prior to this time unless there is a specific terrorist/organised crime threat (Article 5). The UK carrier consultation for our upcoming Data Acquisition orders has concluded that carriers would wish to have the flexibility to provide PNR data earlier than 24 hours prior to departure, according to their varying operating environments. We would therefore wish to see this flexibility reflected in the legislation so that Member States can work with carriers to agree suitable timings in each case.

Data Retention

39. The document requires that PNR data be retained for five years in an active database and for eight years in a dormant database, after which time they shall be deleted. Data held on the dormant database may only be processed in exceptional circumstances. These time periods may be exceeded where data are being used for ongoing investigations or proceedings relevant to the purposes for which they were collected or relevant to the data subject (Article 9). The Government believes these conditions are in line with the principle that data be retained no longer than is necessary. However, we will work to ensure that domestic and EU requirements are aligned and take account of existing legislation governing the relevant Agencies.

Method of Data Transfer

40. The proposal requires carriers established outside the EU to permit a Passenger Information Unit to use the "pull" system of data transfer if they do not have the technology to "push" it to the Passenger Information Unit of the Member State (Article 5). This would necessitate carriers giving Member States access to their system to extract the data. The Government favours the push approach as preferable from a data protection point of view. We will continue to consult with carriers on this issue as part of our implementation, and would welcome the flexibility for Member States to decide how they would like the data transmitted to them in each environment.

PNR Fields

41. The proposal lists the specific PNR data fields that carriers would be required to provide if collected (listed in the Annex to the proposal). Domestic data powers will enable the collection of PNR to the extent it has been obtained by carriers, and each element has been shown to be of use under Project Semaphore. We should therefore not discount the usefulness of any piece of PNR at this stage, and a final list must reflect the balance between privacy and security.

Personal Data/Data Security

42. In addition to the data protection safeguards noted in the above passages, the proposal would also introduce the requirements:

- that any sensitive PNR data collected under the proposed framework decision would be deleted immediately by the receiving Passenger Information Unit or intermediary (Articles 3 and 6);
- that no enforcement action would be taken by Member States' Passenger Information Units or competent authorities only by reason of the automated processing of PNR data or by reason of a person's race or ethnic origin, religious or philosophical belief, political opinion or sexual orientation (Articles 3 and 11);
- that Member States ensure the security of PNR data by implementing appropriate systems and technologies (Articles 12 and 13); and
- Provision for a review of the operation of the framework decision to be carried out within three years of its adoption (Article 17).

43. These are supplementary to applicable safeguards already in existence or soon to come into force. The latter safeguards include the Data Protection Act 1998, which would continue to apply to all UK processing of PNR data, and (when enacted) the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

44. HMG is fully supportive of the inclusion of safeguards and during negotiations will endeavour to ensure that the data protection safeguards applied are as robust as possible. The Government does intend to undertake further analysis to ensure that those safeguards presented offer appropriate data protection without unduly undermining operational effectiveness. In particular, the UK would not wish to withhold its right to process sensitive data under the conditions of the Data Protection Act 1998. We therefore seek to ensure compatibility in the negotiations between UK policy and the EU proposal position.

Regulatory impact Assessment

45. The Commission carried out an Impact Assessment (IA) for this proposal. For the Assessment, two main options with a number of variables were examined—the no change option and the option of a legislative proposal. The Impact Assessment concluded that the preferred option is a legislative proposal with a decentralised system for processing the data, The "no action" policy option does not present any real strength in improving security in the EU. On the contrary, it is anticipated that, bearing in mind the way that this field is currently developing, it will have negative impacts in the sense of creating administrative difficulties stemming from numerous diverging systems.

46. The Government has conducted an Impact Assessment to consider the impact to industry on the UK Data Acquisition Legislation to be introduced in early 2008. This legislation comprises of the power to collect both PNR and API data from carriers in advance of travel for all movements into and out of the UK. A consultation period is now complete and the final IA will be released after internal government clearance is gained. We will write to the Committees when the final version is available.

Financial implications

47. The Commission have not included set costs for implementation of the legislation. They conclude that the financial and administrative burden falling on the community has been minimised through the choice for a decentralised system. Setting up and maintaining a centralised EU system for the collection and processing would entail significant costs. These costs are likely to become clearer after further assessment on the financial impact to industry and Member State national governments.

48. The IA for the UK Data Acquisition legislation provided estimated costs of the e-Borders system in the UK. Our estimated costs to industry (per passenger movement) differ across all carriers, but overall, costs to industry equate to approximately 14p per passenger movement.

Consultation

49. As part of the UK impact Assessment, a full consultation programme was carried out with Industry and other key stakeholders. This included a 12 week consultation period, A set programme of engagement will continue throughout the implementation of the legislation to ensure a fair and equitable roll-out of the UK e-Borders programme. We would encourage an approach at EU level which takes account of the legitimate concerns of the carrier community.

50. The consultation undertaken by the Commission is noted in para 8.

Timetable

51. The proposal notes that Member States are required to take the necessary measures to comply with the provisions of this Framework Decision before 31 December 2010. However, we seek to clarify the Commission's handling of legislation in the early stages of the negotiations. This will give greater clarity to the proposed timetable for the legislation and implementation. We do not expect a conclusion of negotiations until late in 2008 at the earliest.

Annex

Letter from Ms Meg Hillier MP, Parliamentary Under Secretary of State to Vice President Franco Frattini, European Commission

We welcome the Commission's proposal for an EU PNR system and I look forward to discussing it with you in the future. This is a key opportunity to share data in the fight against criminality targeting our borders. We need a permissive framework at the EU level which sets a basis for collection and sharing of PNR and enables our authorities to use this data to maintain the security and integrity of all of our borders.

Such passenger and crew information is key to a fundamentally more effective, efficient and secure border. Stronger cooperation in the EU will increase the effectiveness of our domestic programme and provide wider benefits for us all, while ensuring that we strike an appropriate balance between the right to security and other fundamental values, including the right to privacy.

There were over 200 million passenger movements across the UK border in 2006 and these are rising rapidly. The EU as a whole is faced with similar increases in international travel which brings us great economic and social benefits. However, mass migration also poses challenges of illegal immigration and cross border crime and terrorism.

In the UK, we have run a pilot project, *Project Semaphore*, for three years to assess the value of using both API and PNR data. This has had many significant successes and demonstrated the value of passenger information for bordercontrol and law enforcement purposes and in the protection of the vulnerable. This includes over 1,300 arrests for crimes including murder, rape and assault, the offloading of passengers who would not qualify for entry to the UK and seizure of many false documents, tobacco, and drugs.

Since the projected started, it has covered 38 million passenger movements, and issued over 17,000 alerts. As you can see from these figures, the system only flagged a very small proportion of travellers (one in 2,200) for further intervention, but of those nearly one in 12 were arrested. This shows the extent to which using this data safeguards and enhances the rights of legitimate travellers who do not need to be subject to detailed scrutiny, while detecting successfully the small proportion of travellers breaking the law. PNR also allows the detection of crime that would not have been found using other data sets.

Some examples include:

— Chinese non-documented arrivals. On the basis of PNR data we have offloaded a number of passengers who were subsequently arrested all with forged documentation.

— A two week Semaphore trial on outbound passengers on a ferry route to France identified three suspected facilitators, two tobacco smugglers, one convicted sex offender and one individual under investigation by Kent police. Two forged documents were also identified.

— A passenger was matched by HMRC against one of their drugs courier profiles using essential PNR elements. An alert was sent to the Airline Liaison Officer who intervened at embarkation. His reasons for travelling to the United Kingdom lacked credibility and he was referred to the local police who on searching his baggage discovered 25 kgs of marijuana.

— Location of a murder suspect overseas by linking him to an associate's PNR record.

— Offloading of passengers attempting to smuggle (swallowed) drugs to the UK through PNR profiling.

— Identification of a significant number of facilitators and those using falsified documents through PNR profiling alerts.

We have of course run this pilot project in conformity with UK and EU data protection rules, and with involvement of our Information Commissioner.

Following the success of Semaphore, the UK intends to continue to implement our new borders system. We have this week signed the contract with a technology supplier to deliver the UK's e-Borders system. This will enable the routine acquisition and analysis of both API and PNR data, using our Joint Border operations centre. I would be more than happy to accommodate you or your officials if you wanted to see this technology first hand. I intend to send further examples of the successful use of PNR data, showing in more detail exactly why the PNR element in particular was crucial, in the coming months.

I'm copying this letter to Members of the JHA Council and to members of the LIBE Committee of the European Parliament.

20 November 2007

Letter from Ms Meg Hillier MP, Parliamentary Under Secretary of State, Home Office

I welcome the Committee's interest in the proposed EU PNR Framework Decision and its decision to hold a short inquiry, focusing on the key issue of the scope of the proposal. I am pleased to provide the details below, building on the information provided in the Explanatory Memorandum of 7 December, and in advance of my oral evidence session on 19 March. I understand the Committee has expressed a particular interest in matters relating to the collection of PNR data on intra-EU flights and from rail and maritime carriers; the range of PNR data elements included in the scope of the proposal; the UK authorities entitled to receive PNR data; the transfer of PNR data to third countries; and the ability to collect PNR data more than 24 hours in advance of a flight. I have addressed each of these issues in turn below.

As you know, the draft proposal applies to flights between Member States and third countries and would appear to restrict the processing of PNR data to the fight against terrorism and organised crime. As you will be aware from the EM, the Government wishes to use PNR data to combat a range of illicit activities; to obtain PNR data from intra-EU flights; and to collect passenger data from maritime and rail carriers, as well as from

airlines.[4] This is because persons of interest do not, of course, restrict their travel to international flights and we believe that a comprehensive approach to border management will deliver the greatest benefits to UK citizens and to those people who travel legitimately to, from or through the UK.

Our approach to handling the geographic and transport aspects of scope differs from the way in which we are negotiating over the purpose limitation. The better approach with regard to the geographic scope and the modes of transport would seem to be to accept the restrictions imposed by the instrument, providing explicit provision is included in the text to allow Member States to legislate domestically to process passenger data on journeys by sea and rail and to process PNR and passenger data in respect of intra-EU journeys should they so wish. It would seem sensible and practical to allow Member States to address their particular needs without compelling others to take exactly the same action. For example, we accept that the ability to process data from maritime passengers is irrelevant to land-locked Member States, but may be of great interest to other Member States with busy ports. The e-Borders legislation which came into force earlier this month provides the relevant UK authorities with the powers to capture passenger data from all carriers entering and leaving the UK on all routes.

By contrast, an attempt to rely on domestic legislation to broaden the purposes for which PNR data may be processed, beyond those set out in the EU legislation, could be perceived as undermining the terms of the EU legislation by weakening the data protection safeguards that the instrument aims to put in place. This may give rise to questions over the principle of loyal cooperation. Furthermore, there may also be issues of exclusive EU competence to consider with regard to extending the permitted purposes through domestic legislation. We therefore believe that this issue should be addressed in the text itself.

Annex A[5] to the Commission's draft proposal sets out the nineteen data elements within the scope of the draft Framework Decision. Subject to further clarification from the Commission, the Government does not wish to add any additional data fields but would wish to obtain the same data in respect of crew members. We will inform you if this position changes. However, item 12 in the list at Annex A notes that the General Remarks should exclude sensitive personal data; by contrast, we would wish that officials in the UK's Passenger Information Unit (PIU) with appropriate training and security clearance might manually access sensitive personal data on a case-by-case basis, in line with specific data protection safeguards. Our experience has shown that sensitive personal data can be extremely helpful in eliminating individuals from further interventions because it can sometimes quickly explain unusual features of PNR which may initially appear to be suspicious.

Relevant data protection safeguards could include a prohibition on automated profiling on the basis of sensitive personal data and restricting access to appropriate officials only after a passenger has been flagged as potentially of higher risk. We simply do not profile on the basis of passengers who have chosen, say, a halal or kosher meal, and it is not technically possible to profile on the basis of sensitive personal data in the free text fields. The General Remarks field can sometimes include health data, for example if a passenger is a wheelchair user or has restricted mobility and requires assistance. Other Member States have expressed support for our position on the limited use of sensitive personal data and the Commission has noted that if such data were to be processed under the instrument, the UK's suggested safeguards would seem to be appropriate.

However, the UK believes that the issue of access to sensitive personal data is currently confused in the draft text and it is not yet clear to us what the reference in the Annex to the exclusion of such data would mean in practice. For example, Articles 3(2) and 6(3) require the immediately deletion of sensitive personal data but Articles 3(3) and 11(3) note that no enforcement action may be taken solely on the basis of sensitive personal data, suggesting that such data may in fact be processed. We are keen to obtain clarity on this important matter and look forward to discussing the relevant articles as negotiations progress.

The authorities entitled to receive PNR data from the PIU will be dependent upon the purposes those data may be used for. As you know, the Government considers the current purpose limitation too narrow and we would wish to see this broadened beyond the combating of terrorism and organised crime. The Government believes that authorities with responsibility for tackling a broader range of activities which are damaging to the security and integrity of the UK's borders should also be entitled to receive and process PNR data. Recent e-borders legislation provides that this data may be used by the UK Border Agencies where it is likely to be of use for immigration, police or Revenue and Customs purposes. We would not want this to be restricted by the Framework Decision.

[4] PNR data is a term specific to the airline industry. Personal data collected by maritime and rail carriers are referred to here simply as "passenger data".

[5] See Appendix 3 in the report.

The Government is concerned that the restrictions in the current draft proposal regarding who may obtain "raw" or unprocessed PNR data are unhelpful and unclear. The police forces in England and Wales are, of course, regional with their own intelligence commands based around the country; our Customs service also operates from regional bases. Our police and Customs officers often need to process raw PNR data in their own intelligence hubs in order to enrich that data with existing intelligence to progress criminal investigations as quickly as possible. We have raised this issue during negotiations and the Commission, Presidency and other Member States have been sympathetic to the need to overcome what is essentially an administrative matter. We have made very clear that the appropriate data protection safeguards must still apply wherever the data processing takes place.

The UK supports the Commission's proposal to share data with third countries in line with appropriate data protection safeguards. However, the UK recognises that PNR data may be helpful in combating illicit activities beyond terrorist-related and organised crime. We would not wish to be prohibited from negotiating bilateral agreements with third country partners to use PNR data more broadly where such data sharing was in our mutual interests.

Article 5(3)(a) of the draft proposal imposes an obligation on carriers to provide PNR data to Member States' Passenger Information Units 24 hours before a flight's scheduled departure time, and again immediately after flight closure. However, the final paragraph of Article 5(3) allows Member States to exercise discretion in requesting PNR data earlier than 24 hours in advance of the scheduled departure time under certain circumstances. The UK would like to increase this flexibility in order that we are able to receive PNR data within a 24-48 hour window to reflect our current operational practice.

I hope this information is helpful to the Committee and I look forward to providing further evidence on this important matter on 19 March.

Meg Hillier MP
Parliamentary Under-Secretary of State Home Office

18 March 2008

Examination of Witnesses

Witnesses: Ms Meg Hillier, a Member of the House of Commons, Parliamentary Under Secretary of State, Home Office, Mr Tom Dodd, Director of Border and Visa Policy, Border and Immigration Agency and Mr Kevan Norris, Legal Adviser, Home Office, examined.

Q1 ***Chairman:*** Minister, welcome. Thank you very much for finding the time to come. You have brought Mr Dodd and Mr Norris with you and I am sure that if you want them to supplement any of your answers, the Committee will be very happy to hear from them. We will do our best to release you for Prime Minister's Questions at noon. All I will say to you is that in the days when I was the Government Chief Whip down the other end, I never held it against any Minister who was unable to attend Prime Minister's Questions because of attendance at a Select Committee. Minister, you will realise that this is a short inquiry which the Committee have embarked on prior to a much longer inquiry into EUROPOL. What we are looking at is a follow-up, which I know is a rather tangential follow-up to our earlier report on PNR, but this is a short inquiry into those aspects of the Framework Decision where it appears that Government policy is to treat it as a permissive measure on which the United Kingdom can build a stricter regime. Would you like to make an opening statement or shall we go straight into questions?
Meg Hillier: My Lord Chairman, I would like to introduce Tom Dodd, who is the Director of Border and Visa Policy at the Home Office, and an expert on PNR, and Kevin Norris from the Legal Adviser's team at the Home Office, who is an expert on wider EU law. So, as you indicated, if there are any questions I am unable to answer—or indeed, can answer better than I, although I hope I am able to answer all questions—then they will be able to help. All of this fits in very much with the reforms of our immigration system overall and the introduction of the points-based system that is underway at the moment. My colleague, the honourable Member for Birmingham, Hodge Hill, Mr Liam Byrne, who is the Immigration Minister, has unveiled ten steps towards change over the next 18 months, which is radically reforming our immigration system. Our priority is very much protecting the public and maintaining our borders, so we use our opt-in in Europe appropriately to make sure that we strengthen those aims. But, saying that, we still want to work very closely with colleagues in the European Union and I am making a great effort to talk to colleague ministers from our European partners, as well as European Parliament members. In fact, three or four weeks ago in Brussels I met a number of European Parliament members, including the Baroness Ludford, to talk about this very issue and have invited the LIBE Committee over. We are very

keen to keep up that very direct engagement with Europe because we feel strongly that this issue is one that will help to protect the public and, of course, data protection plays an important role for us in what we are doing both within the UK and with plans in Europe, and it has been the subject of a number of my discussions with ministers. Under the proposals that we have in the UK, we think that by 2010 we can monitor 95% of all passenger movements. We have the technical capability; the legislation has been passed domestically, and we are keen to make sure that we continue to argue the UK's interests within Europe.

Q2 ***Chairman:*** That is very helpful, thank you. You will recall that Article 1 of the Draft Framework Decision gives its purpose as preventing and combating terrorist offences and organised crime, yet Article 11 limits the processing of data for these purposes. You say you want to negotiate a wider scope to include broader law enforcement purposes. Would using PNR data on this scale still strike the right balance between security and privacy?
Meg Hillier: My Lord Chairman, I believe it would. From our own experience of Project Semaphore, which is our pilot, we can demonstrate, and I have been trying to explain this to colleagues in Europe. By using Passenger Name Records and Advanced Passenger Information, we can screen out people who are ordinary, happy, everyday travellers who are not meeting the profile of people who might be a risk to the United Kingdom. That means that we can focus far more closely on the passengers who may be a risk. It is worth emphasising that when we do this screening, it starts when someone becomes a passenger, so it is not data that is held on people and can be used willy-nilly. It can only be used because someone is a traveller and even if a flag comes up that somebody, for instance, has perhaps travelled a certain route and that route historically has been one used by drug traffickers, there would be a manual check by officials from the relevant organisations to make sure that the information then warranted an intervention. So far, our use of PNR data has contributed to interventions and often arrests on a range of activities, including rape, murder and other violent crimes, as well as abuse of immigration law—something that is not within the EU parameters, and PNR has been a major help in that area. One of the other issues, My Lord Chairman, implicit in your question, is about profiling. It is categorically not racial profiling, in fact, from our experience in the UK, fewer people have been stopped because of what they look like because we are using the movements of passengers rather than other data about them. It is based on that movement activity rather than what people might look like, and the inevitable personalisation by immigration officers who have to make an assessment quickly at the border—even with all the training, people are still only human. So, it is blind to what people look like and that has helped in that respect, which certainly European ministers were very interested to learn.

Q3 ***Chairman:*** If I may say so, the controversies over profiling, of which you will be well aware, go much wider than racial profiling, of course.
Ms Hillier: Yes, certainly. You are perhaps talking about religious profiling?

Q4 ***Chairman:*** Well, no, it goes much wider even than that does it not?
Meg Hillier: The information that is used is about passenger activity: everything from buying a ticket at a particular travel agent, maybe in cash, to a particular route travelled, to perhaps a pattern of behaviour so that someone has travelled a particular route very frequently over a period of time. If that threw up a match with some recognised criminal activity from the various intelligence agencies and police who are involved, then that would mean that the group or individual would be looked at more closely, and that manual check would allow any intervention necessary.

Q5 ***Lord Hodgson of Astley Abbotts:*** May I start with a question of clarifying your letter, which probably reveals my ignorance of the way EU law operates. On the second page, in the second paragraph—this is My Lord Chairman's question of building on a framework—you wish "to legislate domestically to process passenger data on journeys by sea and rail". And in the third paragraph begins, "By contrast, an attempt to rely on domestic legislation to broaden the purposes for which PNR data may be processed . . . could be perceived as undermining the terms of the EU legislation". As I understand, in the second paragraph, you are proposing to use domestic legislation; in the third paragraph, as it is currently drafted, it appears to be undermining EU legislation. What have I misunderstood there?
Meg Hillier: We have introduced it domestically; in fact, I put it through the House in a statutory instrument just prior to 1 March, when it came into play. What we are saying is that within Europe, the proposals are not as strong as we would like, but we have had some comfort from the Commission in the discussions that are underway at the moment, in which it has been made very clear that we can use some of the data to tackle criminal issues. We want to see the text tightened to allow us to continue, in domestic law, what we are doing and we are also continually negotiating with colleagues in Europe about the scope. It is interesting that when speaking

to other ministers in Europe about data protection, I have provided them with information about our strong data protection measures. Much of what we are doing is quite popular, but we are ahead of the game with other European colleagues, and to a degree this Framework reflects that.

Q6 ***Lord Hodgson of Astley Abbotts:*** So this third paragraph, in terms, does not state the case; we are able to rely on domestic legislation, because we already are.
Meg Hillier: Yes.

Q7 ***Lord Mawson:*** Would you give us a thumbnail sketch of how it works in practice; the mechanisms of when a person enters the system and how it applies to them, and what they understand is happening to them; do they know what is happening?
Meg Hillier: That is a very good question. What we believe is that this makes it much easier for people who are just travelling normally to travel and not be stopped unnecessarily. So, what happens, for example, Lord Mawson, if you were travelling, at the point at which you buy your ticket and register with the airline, that is Advanced Passenger Information that the airline would have. Then, assuming you are flying, the airline would also collect information at the point of check-in. That information would be passed to the UK prior to arrival, so it could be that you are a dangerous individual and then there would be a match on a watch list against your name. If it was not that, it could be, for example, that you may be travelling a particular route well-known by human traffickers, and that there was a certain method of buying tickets that indicated that route was being taken. That would flag up that there was a match, and there would be a manual check to see if Lord Mawson might be somebody worth stopping and questioning. There may be innocent reasons for that journey, in which case, you would not be stopped. Sometimes people are stopped who may need to be questioned and then released, but most people would be screened out at that point if they were innocent travellers. They key thing is that the legislation is only triggered at the point at which you travel. There are then data protection issues around how the information is used and stored and accesses to different agencies—the police, the Border and Immigration Agency and HMRC in the UK, as well as the intelligence agencies—which have to abide by any data protection if they have made a hit against the system and requested further information. They have to prove they need that information for it to be released to them and they would then hold any information that they had taken out of the system under their own data protection rules within their organisations. I can leave you details on that, if you wish.

Q8 ***Lord Mawson:*** Yes, please. As a passenger, is there any clue given to me that any of that is happening with all my information? I suspect people nowadays are pretty suspicious of any information about them that goes into these databases and generally what they assume is that it is free to anyone and you cannot control it.
Meg Hillier: But it would not be looked up under anyone's name unless there was a reason for that name to be flagged. In most cases, it would be one of the various criminal watch lists that exist.
Mr Dodd: It is information which passengers are giving to carriers anyway, so the PNR is booking data which the carriers have in their systems. When you check in, they have got that API information also, so we are not requiring all the passenger's additional information on their movements, it is existing information which the carriers are then giving to the Government to put into its database, which we then act on only in certain circumstances.

Q9 ***Lord Mawson:*** And the passenger knows that you are doing that?
Mr Dodd: It would be incumbent on the carriers to inform the passengers that as part of the booking process this information may be shared with law enforcement authorities.

Q10 ***Chairman:*** Can I clarify this, because I am still not quite clear. The Explanatory Memorandum says that PNR data should be allowed for "crime-fighting purposes such as immigration and customs purposes". Are you saying that PNR data can be used at border controls when there is no suggestion of a criminal offence?
Meg Hillier: Under UK legislation, we use it for immigration purposes; under the EU proposals, that is not proposed. The EU proposal is simply for terrorism and organised crime. We are arguing that if a murderer is caught through the system, this should be allowed. Sometimes an immigration offence can be part of a bigger picture of criminality. We do not think it is quite as clear cut, but we recognise that within the European model, we need to amend the EU text for purpose and scope—that is what we believe—so that we can rely on our domestic legislation to continue what we are doing within the UK.

Q11 ***Chairman:*** But, are you not faced with a difficult negotiation with the Council, Commission or Parliament if this proposal goes through and you have not been able to amend it? Does that mean it will negative the existing powers you have to use PNR data in the way that the UK can? Are you not in danger of the European Union overruling our present powers?

Mr Dodd: That is clearly why we are seeking to negotiate to provide for what we would wish in this Framework Decision to prevent that from happening. Clearly, there is a risk that the legislation will come out in such a way that we would then be required to change our domestic law, but we want to avoid that happening.

Q12 ***Chairman:*** This is under QMV presumably?
Mr Dodd: No, at the moment it is under unanimity. The instrument could change to co-decision and QMV, depending on the timeline of the introduction of the new treaty provisions.

Q13 ***Chairman:*** But, is there not a danger that because we have opted out of Schengen—and there is a certain amount of ill feeling, as you know, in the European Union about this and this Committee has seen this with regard to Frontex, where we have been told we cannot take part in Frontex because we are outside Schengen—you are likely, if it comes to QMV, to get overruled on this?
Mr Dodd: At the moment, this instrument is subject to unanimity so, in terms of negotiations on it, at some point, should we wish to, we would have the opportunity to veto this. If we climb out under the current arrangements and move into a new treaty and be subject to QMV and co-decision with the Parliament. Obviously, then our opt-in would apply, so we would have the opportunity to opt in, should we want to, or not, into this proposal. Either way, we have a degree of lock on how it would apply to the UK.

Q14 ***Lord Marlesford:*** Minister, in your helpful letter of 18 March, you say, "The e-Borders legislation which came into force earlier this month provides the relevant UK authorities with the powers to capture passenger data from all carriers entering and leaving the UK on all routes." PNR was introduced by the United States initially and they have a very sophisticated form of e-border control, which we do not. My understanding is that it is not expected that we will have proper e-border controls before 2013, or indeed, even later. Am I right, therefore, in saying that it will not be possible to use PNR at British borders before that system is in full force? As I understand it, at the moment, when people come into the United Kingdom and have their passports swiped—as they do now—all that happens is a match against a watch list; there is no record of their arrival kept. Are you telling us that with all the PNR data, if it were to produce a signal of interest, you would have time, between the time of the collection of that data and the arrival or departure—of which at the moment there is no record at all, no swiping, even, of people departing the UK—to put on to the watch list anyone who might be of interest?
Meg Hillier: We already have had this successfully working under our pilot, Project Semaphore. Basically, at the point at which somebody boards an aircraft—some people do not even get on to the aircraft because the check is done at the embarkation point—but the benefit of the system is that the check can be done on that advanced information so that while someone is in the air, on their way to the UK, information can be held. Maybe part of it is the route they are flying, maybe other information about their ticket purchase, as I was explaining to Lord Mawson. When that flights lands, rather than checking an entire flight from a particular destination, which would be a nuisance to other passengers, there can be some identification of people who would then need to be stopped at the border in order to have further questioning.

Q15 ***Lord Marlesford:*** Are you saying, therefore, that as soon as this comes in, even though you will not have e-Borders, you will be able, in every instance you wish to, to add to the watch list anyone who is of interest, in practical terms?
Meg Hillier: Not everyone of interest would be added to the watch list.
Mr Dodd: Firstly, the system we are developing is as sophisticated as the US system. In many ways, I think it is even more sophisticated, because their system focuses very much on terrorism whereas ours focuses on a broader range of crime, terrorism and immigration. In terms of e-borders itself, by 2010, we aim to capture 95% of journeys, both PNR and API data on those journeys.

Q16 ***Lord Marlesford:*** Both entering and exiting?
Mr Dodd: Both entry and exit, yes. The PNR data is captured up to 48 hours in advance of travel, which means that we can run a watch-list or other database checks against that data before the person has even travelled to the UK, so it has utility; it is an add-on to the swiping process at the border; they are two distinct transactions. We are already getting benefit from PNR collection and as e-borders expand, we will get more and more benefit from PNR collection up to 2010. The 2013–14 date is when we will have 100% collection of PNR, which is when the additional 5% will involve small aircraft and people in pleasure cruisers, etc., who are mainly quite low risk.

Q17 ***Lord Marlesford:*** That is very helpful. How many people in total, roughly, are there currently on the watch list?
Mr Dodd: There are about one million entries on the watch list. Just to clarify that, the issue is that when we are doing a watch-list check, which is a one-to-one check, but also through e-borders we have profiles of a suspected drug trafficker who would display certain

traits of behaviour. That individual might not be on the watch list but, for example, we have arrested and prosecuted drug traffickers on the basis of their travel patterns and travel history, not on the fact that their name has appeared on our watch list; the two things are complementary.

Q18 ***Lord Dear:*** Just to clear up a point, I thought watch lists were for named individuals. Am I getting the picture that it is not only named individuals but also it has very strong profiles of unnamed people?
Meg Hillier: Yes, I think so.
Mr Dodd: The Warnings Index has named individuals on it.

Q19 ***Lord Dear:*** Just named individuals?
Mr Dodd: Yes, but we also have profiles that we can run through the JBOC against types of individuals.

Q20 ***Lord Dear:*** But the one million, or thereabouts, that you mentioned, are all individuals?
Mr Dodd: There are a million names on the warning index. Of course, these are people who could, for example, have been found to have overstayed their visa, as well as criminals we are looking for.

Q21 ***Lord Dear:*** Anyone of interest, at whatever level?
Mr Dodd: Yes. Also, over quite a period of time.

Q22 ***Lord Hodgson of Astley Abbotts:*** So, by 2013–14, any question as to whether people have been extraordinarily rendered through the UK becomes clear; we will have all that information as well?
Mr Dodd: That is a good question. I cannot speak on behalf of the Foreign Office. Rendition clearly is not something that I am responsible officially for.

Q23 ***Lord Hodgson of Astley Abbotts:*** We are talking about flights through the UK.
Mr Dodd: The Government has made some statements about rendition. We will be capturing all passenger data by 2014.

Q24 ***Lord Hodgson of Astley Abbotts:*** Anyone who lands in the United Kingdom will be captured?
Mr Dodd: Anyone who lands in the United Kingdom will be captured.

Q25 ***Lord Hodgson of Astley Abbotts:*** Even if they do not leave the plane?
Mr Dodd: Military personnel on military flights are not being captured through e-Borders because they are exempt under military law.

Q26 ***Lord Hodgson of Astley Abbotts:*** Transit passengers?
Mr Dodd: If we have civilians, we have provision in law to capture data on civilians on military flights. We are also talking about passengers who are coming in and out of the country, so a transit passenger who does not actually enter the UK would be caught through e-Borders.

Q27 ***Lord Mawson:*** Does this mean, eventually, when you go sailing off the south coast to France and back that there will be some system introduced for those people so that you are able to monitor where they are going? Is that going to happen?
Mr Dodd: Yes, this is obviously something that we are working on in the e-borders programme and with the supplier, and about which we will be consulting relevant interested parties. What we are looking at is some sort of web-based registration system whereby if you are a sailor and you are going to France for the weekend, you would need to register your details on line, such that we could then, if need be, check that against our databases, etc.
Meg Hillier: My Lord Chairman, it is worth adding that different carriers are at different stages of their ability to collect the data; some are very advanced. The cost, for example, to give you a range of capability: the range of costs per carriers is from five pence per data transfer to 75 pence, which is an average of 14 pence per passenger journey. Different airlines are very experienced at this, but we are having negotiations and discussions with other carriers, including small craft.

Q28 ***Lord Dear:*** The question that concerns us is about the value of PNR in combating terrorism and it has led us to look at the letter, which I think you wrote to Vice-President Frattini, which gave some examples of the success of Project Semaphore. As far as we could see, none of the examples quoted in the letter were for terrorism and only some were for organised crime, the rest were for some sub-organised crime. Behind the question is the supposition that some would hold—not necessarily us—that it is really an expedition to get into things that are not actually terrorism or organised crime. I wonder if you would comment on that.
Meg Hillier: It has absolutely been a tool in tackling terrorism and I think it would be very helpful if we could have discussions, perhaps outside the Committee, about how we can share information appropriately. I have had some difficulty in talking to Mr Frattini about how we can publicly talk about thwarted terrorist attempts or intelligence that has been built up on the basis of this information, of which there is a great deal. I am sure it is not beyond the wit of us all to work out a way of sharing that appropriately with either a member of the Committee or in another way, but not in a public forum. We would be very happy to discuss with you, My Lord

Chairman, how we can work to make sure that the Committee has got that comfort.
Lord Dear: That sounds like a very good idea.

Q29 ***Lord Hodgson of Astley Abbotts:*** You will understand from my earlier intervention that I have a particular interest in rendition and, indeed, in the US/UK Extradition Treaty, where there was an imbalance which was put through in a hurry because it was supposed to be developed as part of the fight against terrorism. The reality was that 30 out of 40 cases so far have been about financial crime. So, I am very concerned about the mission creep in these things. You mentioned that there have been 1,300 arrests and it would be extremely helpful if you could give us a breakdown of what these arrests are so that we can reassure ourselves that similar mission creep is not occurring here.
Meg Hillier: I am very happy to provide you with that. It has gone up to 1,700 arrests. It is difficult to be precise about which is from Advanced Passenger Information and which is from PNR without unpicking every single one, but I am happy to provide a full breakdown.

Q30 ***Lord Harrison:*** Minister, you made an offer to the Commons European Scrutiny Committee to provide case studies of arrests for offences outside the scope of the current draft. Is it possible that we could have those?
Meg Hillier: Again, I am very happy to provide them, My Lord Chairman, but it would have to be on a confidential basis for the Committee, not in public. But if I can just give you a flavour in general terms: if you look at serious criminals, for example, some sex offenders would be outside the scope of the current Framework proposal because an individual would not be part of organised crime and definitely from a UK perspective, that is a very serious issue.

Q31 ***Lord Harrison:*** Right, it would be very interesting to hear the developments on that. You do not want this proposal to restrict the ability of Member States to collect and process data for other modes of transport. Do you envisage using PNR data to cover land and sea transport—I think you alluded to that earlier—and would this include the Channel tunnel and rail transport by Eurostar? Could you also reflect on whether this would be practical and proportionate? I rather link that to the answer you gave in the third paragraph of your letter of 18 March to Lord Grenfell where you say, "It would seem sensible and practical to allow Member States to address their particular needs without compelling others to take exactly the same action." So, you are looking to get a kind of "bespoke" response in terms of Member States appropriate to their particular concerns. In some ways that seems very wise but is there a danger of some confusion or uncertainty about what is operating in terms of the decision to interact with the Framework? Might there be a source of confusion there?
Meg Hillier: I do not think there should be confusion. Some of it presents operational challenges for those carriers, as I have indicated, and so we are working closely with the different carriers. To make sure that this works effectively, we must be careful not to have any loopholes. As Mr Dodd said, we aim to have 95% onto our system by 2010 and that last 5% is, we have assessed, a fairly low risk. Nevertheless, when something is a loophole it becomes inevitably the higher-risk route and potential route for people who are undesirable to enter the country. We are working with those carriers now and I do not think that it should be difficult. As I indicated, there is a differing level of technical capability within the different carriers and sometimes within the different travel industries and that is what we are currently working through with those carriers.

Q32 ***Lord Harrison:*** So, that embraces the answer to the Channel tunnel and the Eurostar?
Meg Hillier: Yes, the Channel tunnel and Eurostar will be included in the PNR.

Q33 ***Chairman:*** Can I go back to Semaphore. Could you give us some idea, looking at those 1,300 arrests, what proportion of those you would not have been able to make if you were only operating under Advanced Passenger Information systems?
Meg Hillier: It is very difficult to differentiate without going through every case that we have picked up and pulling out exactly how it is done. Often it is a pool of information, so I cannot honestly give the answer to that. All are useful, but it is the combination of data that helps us solve that.

Q34 ***Chairman:*** Perhaps you could try and help the Committee a little; if you cannot be precise, just give us broad parameters.
Mr Dodd: For example, in 2007, we denied boarding to 58 people on the basis of PNR only. But, in most cases, as the Minister said, it is a "milkshake" approach from PNR data as to a number of other factors and information from which we have to make an assessment, which then leads to off-loading or on-board charging or prosecution.

Q35 ***Lord Mawson:*** With regard to that, how much work do you put into particular individual cases? My experience is on very large schemes and it is sometimes helpful to put a lot of detail into micro-examples of what exactly happens and what you know from one or two examples so that you understand what is happening more widely. What

effort is put into really getting underneath the detail of one or two of these examples.
Meg Hillier: Ministerially, I am repeatedly asked for real-life examples, partly because scrutiny of all sorts helps, appearing before the Committee today obviously helps, but actually my work within Europe—as I am the Europe Minister for the Home Office—means that I am constantly asked that question. I am doing that from a Ministerial level, but Mr Dodd can explain other mechanisms.
Mr Dodd: We have a Joint Border Operations Centre in London where this information is collected and assessed. We have a number of officers who work there, who are looking at the data, looking for patterns in the data and issuing alerts. They can do some digging, but that might then be referred to a regional unit, which will do more intensive mining of the information, and they will dig quite far into this data. For example, in the PNR data, one of the fields is the credit card number used by the person who bought the ticket or tickets. That credit card number could have been used in a number of different cases by a suspected criminal to procure transport or some other service. The person who has bought a ticket may link himself or herself with some other people of interest and so you have a pattern which is essentially the pattern generated from the examination.
Meg Hillier: The Committee is very welcome to visit the Joint Border Operations Centre, if you feel that would be useful, because you can see what happens there. In fact, the LIBE Committee is coming to visit it.

Q36 ***Chairman:*** That could be very useful. Where is it?
Mr Dodd: It is near Heathrow Airport.

Q37 ***Lord Marlesford:*** I want to ask a very practical question, which arises from what Lord Harrison was saying in the first instance. PNR was introduced primarily as a system—and it is not the only system that the United States uses—which is used for air travel. The essential difference between the Eurostar, i.e., rail travel, and to a lesser extent, sea travel, and air travel, is that you have, in practice, to book ahead for air travel but you can turn up at a railway station and buy a ticket—you may have to pay a bit more than if you book ahead. I cannot see, in practical terms, how conceivably any PNR data from the process of buying a ticket for the Eurostar could be put usefully, for that journey, into your watch list.
Meg Hillier: Advanced Passenger Information, which is already collected, provides us with at least the length of the journey to check someone's information. That, on its own, can be very useful and we are talking very closely with those carriers about how that is done because we recognise and understand that people want flexibility of travel. You can still turn up to an airport and buy a ticket, so there is precedence for dealing with this.
Mr Dodd: Based on rail and sea routes, many people book ahead, so the number who turn up and go is a minority. There is a pressing need for us to have PNR data because obviously the journey time is quite small; the journey from France to the UK by train is about half an hour. If somebody turns up and buys a ticket and they are queuing for half an hour to get on that service, that still gives us another half an hour to flush that data through our system and get a match. The more warning we have of travellers, the more we are able to screen them and prompt interventions if they are required.

Q38 ***Lord Marlesford:*** But you do not anticipate that the introduction of PNR for such journeys will in any way inconvenience passengers. You mentioned credit cards, if somebody who does not wish to give more information than the minimal uses cash to buy the ticket , all they will then have to have is their passport, or ID card.
Meg Hillier: Equally, for many advanced purchases that could be the case.

Q39 ***Lord Marlesford:*** Sure, but the point is that the timescale is quite different; you turn up at the place and get on to the plane.
Meg Hillier: It is a challenge and we have got to try and get that balance about the convenience for the general passenger and risk, and making sure that we are not tightening down so much that it makes it impossible for the general passenger to travel freely. We are having quite intense discussions with these carriers to make sure that we get the balance right. When you travel on an aircraft now, most people are aware that they go through security screening, their bags are checked and they probably would expect that, even if they are not fully aware of it—though we are working with airlines to make sure that they are providing information about what happens to the data—people want to be reassured about that. If it is not happening effectively on trains, then we have a duty to protect the public and make sure that we get some good solutions. So, it is a case of "watch this space", My Lord Chairman; it is being worked on, but we have not quite got a resolution.

Q40 ***Chairman:*** Yes, but you keep talking about a balance. It seems to me that on one side of the balance you have got an effective and as good a monitoring system as you can get, and at the other end of the balance you have got a great big black hole, where someone using Lastminute.com and people who just line up—I think we have all at various stages in our lives got on a train or a plane at the last minute—and following what Lord Marlesford was saying, I do not

really follow how you can prevent this unless you say that you cannot book less than an hour ahead.
Mr Dodd: We cannot have 100% of what we want. It would be unreasonable to require passengers to turn up two hours before they travel in those circumstances. What we are trying to get is as much data as we possibly can. In terms of the maritime and rail carriers, we are working with them to see the best way in which we can collect that PNR data.
Meg Hillier: It cannot be as far in advance but, for example, if you take a ferry, very rarely does someone turn up to a ferry and just go very quickly, because of the queuing mechanism that they have—the incoming ferry has to arrive, disembark and then embarkation takes place. It may become more challenging to turn up and pay in cash, depending on the outcome of these current negotiations, and in fact in many environments—I do not know when members of the Committee last tried to buy a rail ticket but you have to hunt around for a machine that will take cash only, at Victoria, for example—it is very much card-based. Those kinds of mechanisms can make that Advanced Passenger Information more effective. That is probably where we will end up with a balance; while not restricting the rights of passengers to be able to travel relatively freely and easily, that will be where the negotiation comes down, but I would not want to predict the outcome.
Mr Dodd: If our systems detect an individual turning up repeatedly at the last moment and not booking in advance, then interest will be triggered in the individual and we may then take secondary action to look at that person or that vehicle as a consequence.

Q41 ***Lord Hodgson of Astley Abbotts:*** Is this wish to hold the traveller in the field for as long as possible part of this background to the Terminal 5 decision not to allow people to fly if they have not arrived 25 minutes before a flight?
Meg Hillier: I have no knowledge of that at all. I have not had any involvement in those discussions. Certain airlines are very strict about their check-in times and I suspect it is more to do with the airlines but I am not au fait with the details.

Q42 ***Lord Marlesford:*** We have the impression that you are trying to extend the system so that it covers intra-Member State travel as well. That, presumably, in terms of Schengen, where there is no checking in between States on land journeys particularly, it is not doable; where there is no control, there is no record.
Meg Hillier: For flights, it is possible, and that is really the main focus because, clearly, criminals do not restrict their activities to the boundaries of Europe, but they will travel within. That flight information is handled in very much the same way as international flights so that people buy their tickets in advance and Advanced Passenger Information will be available. For Eurostar, for example, there will still be a degree of checking between Paris and Lille.

Q43 ***Lord Marlesford:*** It is the "weakest link" argument; people will be well aware of where you can check and therefore will focus on where you cannot.
Mr Dodd: The reason why we have retained our border controls and we are not part of Schengen is precisely so that we can screen and control people coming to the UK from mainland Europe.

Q44 ***Lord Marlesford:*** Yes, but my understanding is that you are seeking to amend the Commission's proposal so that it includes something that is really not included.
Meg Hillier: We are trying to get a balance. Clearly, there are going to be different interests. We are trying to get a common European framework that protects Europe, while allowing individual Member States to do what works best for them. For example, the landlocked countries will not have any interest in maritime borders. We want it to be permitted to allow the UK to continue to do what it does. I have had some very interesting and fruitful conversations—I do not want to declare them publicly on the record—with European ministers who are very interested in what the UK is doing. We have had a number of people visiting the Joint Borders Operation Centre and more have been invited and are planning to come. The Minister in Ireland, Mr Brian Lenihan, is very keen to meet the LIBE Committee when they visit and in joint hosting by ministers, because the Irish feel very strongly about this issue also.
Chairman: Just to comment on what Mr Dodd said with regard to the UK's exclusion from Schengen, you may recall that in our Frontex report we endorsed and supported the Government's policy in excluding the UK from the Schengen Agreement.

Q45 ***Lord Dear:*** Minister, I have a couple of questions, inevitably, about data protection. There have been many much publicised and embarrassing breaches recently and against that background, I wonder if you can satisfy us that the data that will be collected in and concerning the UK will be kept securely and whether you have a view about how our own information will be kept abroad, and whether that will be secure also? And if you are satisfied, why?
Meg Hillier: It will certainly be held very securely; we have to meet a number of strict requirements. I am very aware of the sensitivity because of the data loss at the end of last year, so not only do we need to do it, but we need to demonstrate that to the public. Data will only be released if they can prove that there is a valid need to have that data. Under the Framework, this is one of the key areas of

debate about making sure that the data protection is applied appropriately. I have had some very interesting discussions in Europe about the data protection framework that currently exists and whether that is enough to cover this issue, or whether there needs to be some greater comfort for some countries. We have passed e-Borders legislation through without any party in the Commons disagreeing with our proposals; the legislation went through straightforwardly last month. What I am hearing from colleagues in Europe is that a number of them were worried that they would not be able to get this through their parliaments and we need to look at that very closely to make sure that we have that effectively worked up. The Commission's proposal includes a number of articles to ensure safeguards and we support the majority of those. That includes retention periods, automated data processing, notification to data subjects—it is important that people know what information is held on them—and requirements to ensure data security. As I said to other Member States, data transferred across an EU border will be under the Data Protection Framework Decision the terms of which have already been agreed.

Q46 ***Lord Dear:*** Do you find our non-membership of Schengen causes problems in this field? With every country the holding of data and the relationships around that are inevitably sensitive. Do they view us as being different? My Lord Chairman has already mentioned the differences we spotted with Frontex and I wondered if it has come onto your screen in this particular area.
Meg Hillier: The mood music that I feel as a representative of the Home Office and the Government when I am in Europe is that I need to work particularly hard to prove the UK's common interests in Europe because we are not in Schengen. I make a particular point of working very closely with and talking to ministers to stress that while we are not in Schengen, we have some shared interests. While we are not in Schengen we explain what the reasons are for that. The reasons are quite clearly understood, certainly in the operational discussions I am having with colleague ministers. On this issue, it has not been a particular concern. I presented to ministers, when we went to an informal Justice and Home Affairs Council in Ljubljana, Slovenia, in January, and the discussion, with no rankle from colleagues around the table about the UK's position, rather interest in how we were doing it, could they visit, what were we doing about data protection and what would happen with the timescale and the practicalities. So, we were very much bedded into practical discussions rather than the issue of the UK's position on Schengen. I have found that once we start discussing practical issues and solutions, politicians are politicians, and in the end ministers want to be able to go back and satisfy their parliaments and their electorate and they are looking very much at that, so the practical issues appeal to the political mind.

Q47 ***Lord Dear:*** Taking the data issue that little bit further, inevitably there will be a wide range of UK agencies that will have access to the data. I wonder if you could give us a list, either now or later, of the UK agencies that currently have access to the data. If we are right in the assumption, why is it wider than in other Member States?
Meg Hillier: I will give you what I know, off the top of my head, but I will make sure we write to you so that it is clear. Currently, the Police, the Border and Immigration Agency, HMRC and the security agencies have access to the data. Mr Dodd may be able to answer about what is the equivalent in other European countries.

Q48 ***Lord Dear:*** Do you think Work and Pensions have access?
Meg Hillier: They could. As with other data, it is the same rules that apply; if anyone else wanted to have access, they would need to have a reason to ask for access; they might go through the Serious and Organised Crime Agency, they might raise possibly with the Police. It is possible, I suppose, that the DWP could have a criminal issue that they would raise with the Police, who would then access that as a check against and if necessary there would be discussions about release of that data on the individual.
Mr Dodd: We have been discussing with other government departments the utility of this data. Obviously, in terms of the DWP, it is a question about benefit fraud and people who are out of the country when they are claiming benefit, etc. To my knowledge, we are not doing that at the moment but we may do in the future.
Meg Hillier: It is worth saying that no one can "mine" the data. No organisation or individual without clearance can go in and start looking up individuals by name or finding things out; it has to be that they have a concern that a person has done something and therefore they are asking for information about the individual, there will be a check against them and then that information may or may not be released, depending on whether it is felt appropriate.

Q49 ***Lord Dear:*** From what you say, those four agencies would be mirrored exactly in other EU countries.
Meg Hillier: I cannot tell you precisely what every other EU Member State is doing.

Q50 ***Lord Dear:*** But it is more or less in step.
Meg Hillier: Yes. The big difference from the UK's point of view is that the Borders and Immigration Agency use it as an immigration tool, and in the European Framework it is not proposed as that, partly because of our relationship with Schengen.

Q51 ***Lord Hodgson of Astley Abbotts:*** When we send information, we have our watch list and are dealing with our European colleagues, do we run on any check on speciality? That is to say, the issue that bedevilled the Extradition Bill Act was the issue of whether a crime committed, which was something that was not a crime in this country but was a crime elsewhere, and how the extradition would work. Are we sending information, do we know what information is being requested and why? And if so, do we run any speciality check for offences which are offences in certain countries in continental Europe and not offences here, or do we just send the information without any check?
Meg Hillier: No data is just released, there have to be some checks –you are thinking of Holocaust denial perhaps? I am not sure but perhaps Mr Dodd can answer.
Mr Dodd: It is like any legal aid, mutually-policing request, if they are asking to check our database, whether it is for fingerprints or whatever, they would have to come up with the justification as to why they want us to do that, and it would be dealt with by the authorities in the normal way.

Q52 ***Lord Mawson:*** Article 8 of the proposal limits the onward transmission of data to third countries. What changes would be needed to ensure that the UK retains its current powers for the onward transfer of data?
Meg Hillier: We believe that the purpose limitations proposed are too narrow because the current restrictions would prevent co-operation with third countries to catch, for example, the serious criminals that I was talking about earlier, whose crimes are not connected with terrorism and they are not part of an organised conspiracy, for instance, the single sex offender that I highlighted. We also believe that it would be important to safeguard our ability to enter into bilateral arrangements with third countries on this. But we want a standard at least as high as the Data Protection Framework Decision and we believe that the Data Protection Act is comparable. We are discussing with EU partners a shared code of practice and have invited them to see the Joint Borders and Operating Committee to make sure that we deal with this issue. When I met MEPs a few weeks ago with Sophie Int'Veld, the Rapporteur for the LIBE Committee, and Baroness Ludford, among others, this was an issue of great discussion and debate, which is one of the reasons the LIBE Committee is coming to visit. We are also going to provide them with information about our data protection approach so that we can bottom this one out across Europe.

Q53 ***Lord Mawson:*** Obviously, we are all very sympathetic to the present situation and the need for government to know a great deal more about us and about these situations; we understand that. But, do you foresee a day when it might be necessary to reduce the level of government knowledge about all of us as individual citizens and we might be given again more private space?
Meg Hillier: That is a big question, and I am the Minister responsible for identity cards and data across the Home Office, in many respects. Talking to members of the public on the doorsteps of my constituency, for example, most of this information is not information that people will see or even know about. It is triggered at the point of travel. It is about you as a traveller and it enables and supports the traveller to carry out their journey easily. People cannot mine into that, so it is sitting there but not necessarily used and no one can look into it unless they have a good reason. It is about balance between privacy and safety and I would say, as a Home Office Minister, that safety of the public has to be paramount. What I would be concerned about is if we had a system where everybody was being checked going through an airport, which obviously would not be workable and would cause great disruption for passengers. I think this is proportionate because it means that most people can carry out their journeys quite reasonably and manage without knowing what is happening. In effect, they are entitled to know and the airlines should be telling them about what the data is being used for but it is not going to affect them on a day-to-day basis because most people will just go through and will not even be matched against the lists; there will be no flag, no problem. Those who are flagged will be looked into in more detail, and I think that is proportionate.

Q54 ***Lord Marlesford:*** I would like to come back to profiling for a moment. Presumably the object of the whole exercise is that you identify people in whom you might be interested and the only way you can focus your attempt is to use all the information you have, and presumably profiling is the essential part of the whole system and must be done. You indicated at the beginning that there were certain aspects of profiling that you were rather worried about but if, for example, you take Her Majesty's Customs, they are trained very much to profile on a non-electronic basis—because they do not have it—appearance, behaviour and all the other things. There would not be restrictions on the extent to which you can profile from any of the data you are collecting under PNR, surely?

Meg Hillier: All these interventions will require a manual check by trained officials in the relevant agencies, but the point about the profiling that takes place this way is that it matches clearly to patterns of behaviour and, as you indicated, behaviour is one of the mechanisms that indicate that someone may be of interest. What does not happen, for example, is that people are not profiled because they ordered a halal or kosher meal on an aeroplane; those things would not be a reason to stop somebody—it is about the pattern of behaviour. In answer to your direct question, trained officers are still able to use their training, but the point about PNR and API is that it will flag up people of greater interest so it saves them stopping people who are not of any interest. We have found that the number of people stopped, for instance, from an ethnic minority background has decreased since PNR was introduced—in the pilot, anyway.

Q55 ***Lord Marlesford:*** Where people come from and what passport they hold may be very relevant.
Meg Hillier: Yes, but that information would be picked up through PNR, and indeed, it may be a route that someone has travelled and their national passport. When I visited the Australian immigration system in Sydney airport last summer they were showing me some of the forged documents—pity anyone Greek during that fortnight last summer, because a number of forged Greek passports were picked up, so through their systems for a couple of weeks they were stopping all people with Greek passports. That was proportionate; I think it was very tough for the legitimate Greek travellers, but it was because they had picked up a risk. That information is available through PNR; it does not require only a manual check. The point is that the manual check of the information might stop some of those individuals being stopped but it will also help identify those who do need to be stopped and questioned.

Q56 ***Lord Marlesford:*** But in general, the stop process depends crucially on what is now called a watch list and which, when you have full e-Borders control, will be something rather broader?
Meg Hillier: Yes, that is right. Currently, the watch list is individual and the PNR proposals that are going on now within the UK means that people with a pattern of behaviour. Let us be really clear and it may be worth laying out: it is where people bought their ticket; how they paid for it; their passport; the airline they travelled with; the route they travelled; and maybe people they travelled with. It may be worth giving an example of one case where two suspected people trafficking facilitators were identified at the border which was as the result of a watch list check using just Advanced Passenger Information data at check-in. They produced a copy of an itinerary, but it was suspected that they had travelled by a different route and were attempting to conceal their link with other individuals. Not long after that, four passengers were stopped at a border control with false documents. By checking the PNR data—this is where it really came into play—it was possible to demonstrate that all six passengers had travelled together, and that caught people traffickers.

Q57 ***Lord Marlesford:*** You are talking about America, now, presumably where they have got it.
Meg Hillier: No, that was our own Project Semaphore.
Mr Dodd: We capture at the moment something like 30 million passenger journeys a year already—that is PNR and API on a number of routes.

Q58 ***Lord Marlesford:*** Which is what percentage of the total?
Mr Dodd: It is something like 15%.

Q59 ***Lord Marlesford:*** Fifteen per cent already, and you will have 95% by the end of 2010.
Meg Hillier: Yes.

Q60 ***Lord Marlesford:*** And next year?
Mr Dodd: Next year, we want to have the majority, over 50%, by next April.
Meg Hillier: We will happily send you a schedule of our targets.

Q61 ***Lord Dear:*** Back to data protection, although I think you might have touched on this before. Under Article 11, the processing of PNR data is governed by the Data Protection Framework Decision. As I understand it, the Decision itself is quite limited in scope and I wondered if you consider that the regime that will be in place, or is in place, is adequate.
Meg Hillier: This is the subject of some discussion at the moment, but the provisions of the Data Protection Framework Decision only apply to the processing of PNR data, where it is being or has been exchanged between Member States. It would not apply to data that we are currently collecting from British Airways to our systems and then processed solely within the UK. That domestic processing is subject to our own data protection laws, not to the Framework. That is something we have drawn to the attention of the Commission and we expect that the next revised version of the proposal to clarify the scope of the Data Protection Framework Decision to reflect this. It is, in a sense, a technical point because all Member States have undertaken to ensure that the standard of data protection regarding domestic data processing is higher than, or at least matches, the Data Protection Framework Decision.

Q62 ***Lord Hodgson of Astley Abbotts:*** Still on the issue of data protection, there appear to be arguments that the Framework Decision applies only to data processed by public authorities which are responsible for law enforcement. There are, of course, the data protection provisions for private sector bodies—the airlines and their intermediaries who supply them with services. Where are we on that?
Meg Hillier: We have got some substantive discussions still to have with the Presidency and other Member States on this issue. In the UK, the Data Protection Act applies to private entities, including airlines and specialist IT providers, and the Act would apply to all the data processing by private UK bodies and those engaged in the process. We also expect that data security standards imposed on Passenger Information Units by the draft instrument to extend to a large extent to the carriers transmitting PNR data.

Q63 ***Lord Hodgson of Astley Abbotts:*** To a large extent?
Meg Hillier: Yes, they would have to adhere to the Data Protection Act.

Q64 ***Baroness Garden of Frognal:*** You say that the proposal respects fundamental rights. It appears that the European Data Protection Supervisor categorically disagrees with this. I wonder if you have considered his detailed reasons.
Meg Hillier: We have and we do not disagree with many of the fundamental premises of his report, for example, we want measures to be proportionate and balanced in terms of privacy rights. We were encouraged by his view that the fight against terrorism could be a legitimate ground to include exceptions, but we disagree with his analysis because we think that in terms of necessity PNR data has helped to identify high-risk criminals—I have given one example of that, and I could give others—and we think that is very helpful. It has contributed to a number of arrests, 1,700 alerts[1] so far and then arrests arising from that, on our pilot alone. The intelligence agencies are very clear that PNR is a very valuable tool. My Lord Chairman, I think we have already provided some hard copies of case studies to the Committee.

Q65 ***Chairman:*** No, I do not recall seeing them.
Meg Hillier: Apologies; I will make sure that happens. We think that what we are doing is proportional to the risks involved and causes least disruption to individuals. In terms of their privacy, we think that it is a reasonable balance to have struck, but we do have some disagreements.

[1] See correction in Q 67.

Q66 ***Baroness Garden of Frognal:*** Could you tell us what the views are of the Information Commissioner?
Meg Hillier: We have been working very closely with the Information Commissioner on this issue. One of the reasons why I am sharing information with European colleagues about our work on data protection is because we have had some very good dialogue with the Information Commissioner on this issue. We also have a six-month review, My Lord Chairman, and it maybe that the report you are doing will contribute to that. The Committee is obviously very welcome to come back and look at this issue. We do not ever feel that we are at a completely fixed position; we have the legislation in place; we are using this; we are discussing and negotiating in Europe, but we are open to constant improvement and renewal, and the data protection issues are pertinent. It is very important that we have the protection of the Act but, even within that, we want to make sure that we are doing what is proper and appropriate in order to make sure that we can maintain this and maintain the balance of privacy for individuals concerned.

Q67 ***Lord Harrison:*** Out of those 1,700 alerts, do you know how many arrests there were?
Meg Hillier: There were 20,000 alerts and 1,700 arrests.
Lord Harrison: That is most helpful.

Q68 ***Baroness Henig:*** We touched earlier on the fact that if the Treaty of Lisbon was in force the measures would need co-decision and we had a discussion about that. You very helpfully mentioned discussions that you have had in Europe, which I assume have been within the framework of the Council of Ministers. I wondered what steps the Council was taking to involve the Parliament more closely, in view of what might happen in the future.
Meg Hillier: I met a number of MEPs, as I mentioned, and they made it very clear to me that they felt the need to discuss the issue with ministers, so the very next day I spoke to French colleagues urging them to arrange better contact between ministers and MEPs. They were very keen to do that, so we are hoping that will happen at the beginning of the French Presidency. I was also talking to a number of ministers individually, encouraging them to talk, not only to their own national MEPs, but to some the key members of the LIBE Committee in particular, because of their interest, to talk to them about this and make sure that there is proper engagement. I was very struck by the intelligent and informed knowledge of the members that I met and their willingness to make it work and make sure that their concerns were properly addressed. I have absolute

sympathy with that desire for engagement; I think that is what politics is about and we are hoping that the LIBE Committee will come to the UK fairly soon to see for themselves what is going on and that discussion will continue.

Q69 ***Chairman:*** Minister, you should never have been struck by the intelligence and the information that is held by members of the European Parliament. *Meg Hillier:* Yes, you are right. I expected it, but it nevertheless impressed me. I have been talking to the Danes—I am not sure it is going to happen—but we are looking to do a joint presentation to the LIBE Committee so that the Committee gets the opportunity to question, particularly the UK, because we have been doing this, so they get that opportunity to get in-depth with the practical side of it as well as the more theoretical discussions.

Chairman: Minister, we have had the pleasure, also, of having Lady Ludford, who is a Member of the European Parliament, sitting quietly and politely at the back of the room, who I am sure has taken a great interest in what you have told us. Thank you for coming and for being so clear and helpful. Thank you particularly for offering private briefings on these matters. That is very helpful and we will be in touch with regard to that. I said that we would do our utmost to release you in time for Prime Minister's Questions; there are five minutes to go and if you run, you would just get there in time, although I suspect, having some experience of the House of Commons, that Questions will be more involved today on Treasury affairs than Home Office affairs, although I may be wrong. Thank you for coming and thank you to your colleagues. Mr Norris, you have been sitting quietly there and we have not heard from you; but thank you all very much, we much appreciate this.

Supplementary evidence by the Home Office

I wanted to thank you for inviting me to give evidence to your Committee on 19 March with Meg Hillier MP and Kevan Norris on the European Commission's proposal on PNR. This draft instrument is an important dossier for the Home Office and we welcome the opportunity to provide further detail on its contents and implications.

During the evidence session, the Committee requested further details on the arrests made under Project Semaphore in 2007 and these are attached. However, we are unable to provide a full breakdown of arrests resulting specifically from the processing of PNR data. This is because PNR is frequently used in conjunction with other passenger data and intelligence, making it extremely difficult to isolate its specific contribution to the outcome of a case. Sometimes a particular piece of evidence can quite clearly make a critical difference in obtaining a conviction, for example, a key witness statement or forensic evidence, but very often it is the collective impact of the contents of the prosecution file that determines the outcome of the case. PNR data is one of a number of very useful investigatory tools. We do not, by contrast, try to assess the value of door-to-door questioning or covert surveillance simply in terms of convictions. Furthermore, it is not the objective in every case to try to obtain a conviction. Approximately 200 alerts per month are issued to monitor the movements of sex offenders, and under certain circumstances, our authorities choose to apply administrative sanctions, rather than pursue criminal charges.

I expand below on some of the more substantive issues that were raised during the course of the evidence session. These issues cover the distinction between Advance Passenger Information (API) and PNR data; the UK's e-Borders legislation; the possible impact of the Commission's proposal on our domestic legislation; and the data protection provisions in the Commission's proposal.

Distinction between API and PNR Data

PNR data comprises reservation data collected by carriers for commercial purposes during the booking process, at check-in and from any updates made in between. The data covers up to 19 data fields including passenger name, travel itinerary, contact and billing information and so on (the full list of data fields forms Annex A[6] to the Commission's proposal). Under the UK's e-Borders pilot, Project Semaphore, we have been processing PNR data on carefully selected routes since October 2005. The Government has never placed any obligation on carriers to collect specific PNR data and usually less than half of the 19 data fields are collected.

By contrast, API data contains biographical information from the passenger's travel document and the unique service information used by the carrier to identify each particular routing. Under e-Borders, we will receive PNR data 24–48 hours before the scheduled departure time; API at check-in; a second supply of PNR data once the carrier is satisfied those data are final; and separate departure confirmation to confirm those

[6] See Appendix 3 in the report.

passengers who are on board once the aircraft doors are sealed. This process allows as much time as possible to run the PNR data against a range of profiles, but also ensures that we have all of the data available; many of the passengers of greatest interest to our authorities purchase their tickets very shortly before travel.

PNR data is checked against a number of profiles developed using evidence gained from arrests, customs seizures and police intelligence. Officials will then manually access, on a case by case basis, those passengers' PNR data flagged by our automated system as a profile match, and will carefully assess whether to issue an alert; make an intervention; or decide that the passenger does not appear to pose a risk and so take no action. The profiles are constantly reviewed and updated. The production and review of profiles is a process based on intelligence and evidence exchange between officers in JBOC with particular expertise in profiling and officials from the JBOC authorities.

PNR data is very useful in identifying potentially high risk individuals whose identities have not come to the adverse attention of UK authorities; by contrast, API data is particularly useful where an individual has already done so. API data is taken from the travel document itself and so spellings of names and the date of birth are transcribed more accurately; it is therefore API data that we use to check against our watch lists.

Project Semaphore collected API data on a far wider range of routes than those on which PNR data were collected. Under e-Borders, we aim to collect API data on 95% of all passenger movements, to and from the UK, by December 2010. We aim to collect PNR data on far fewer passenger movements, focusing only on the higher risk routes to and from the UK. We believe that this limited collection of PNR data, focusing on those routes of greatest interest, helps to illustrate the proportionate nature of our use of PNR.

e-Borders Legislation

Our domestic legislation underpinning the e-Borders programme enables the UK to process PNR data for counter-terrorism, police, immigration and customs purposes. This legislation also permits us to collect data from all carriers—air, sea and rail—on all routes, including intra-European journeys.

Under the Duty to Share Order, the Police, the UK Border Agency, HMRC and the security agencies have access to PNR data. This list may well appear to be more extensive than in other EU Member States because of the organisational structures in the UK. For example, the remit of the French National Police covers policing, intelligence, customs and immigration functions whereas the UK has a greater number of separate agencies dealing with a more restricted range of functions.

The Commission's PNR Proposal: Scope

The Commission's proposal for the use of PNR data for law enforcement purposes has a more restrictive scope than that provided for under UK legislation. The proposal limits the collection of PNR data to flights to and from third countries, into and out of EU Member States, and restricts the processing of PNR data to the combating of terrorism and organised crime. The UK Government considers it necessary to broaden the scope of the draft instrument to ensure our border management programme is not undermined, and hence put at risk the security and integrity of our borders and the safety of all those who travel to, from and through the UK. Criminals do not restrict their travel to international flights and offences aside from terrorism and organised crime can also cause great harm to our society. There are three distinct aspects to the question of scope, namely purpose limitation; geography; and modes of transport. We intend to manage these issues in two different ways.

Geographic and Modes of Transport Scope

We can accept the restrictive scope of the draft EU instrument with regard to international flights and air carriers, providing there is explicit provision in the text to allow Member States to legislate domestically to extend the geographic scope and the modes of transport involved. Should the Commission proposal be amended to include this provision, we understand we would be able to rely on our domestic e-Borders legislation to collect PNR data on all routes and from all carriers. (On this point, it is also worth noting that the collection of PNR data for law enforcement purposes from non-international flights would appear to be compatible with the Schengen acquis; PNR data collected on intra-EU flights could be checked by Schengen states for law enforcement purposes but not for immigration.)

Purpose Scope

In contrast, an attempt to rely on the domestic legislation to broaden the purposes for which PNR data may be processed, beyond those set out in the EU legislation, would appear to pose a higher risk. Such action could be perceived as undermining the terms of the EU legislation by weakening the data protection safeguards that the instrument aims to put in place (the purpose limitation is itself a data protection safeguard). This may give rise to questions over the principle of loyal cooperation and there may also be issues of exclusive EU competence.

We do not believe this would in fact undermine an appropriate standard of data protection—indeed, we consider that Project Semaphore has demonstrated how PNR data may be used to combat a broader range of illicit activity while still maintaining appropriate data protection safeguards. However, to avoid any risks on this front, we are seeking to amend the text of the proposal to broaden the purposes limitation within the EU legislation itself. This issue has already been raised as an important issue for discussion by a number of Member States and we expect substantive negotiations to begin in this area shortly.

Data Protection

During the evidence session, the Minister referred to the data protection framework that would govern the processing of PNR data. The EU Data Protection Framework Decision (DPFD) will shortly come into force and will govern the processing of personal data (including PNR data) which is transferred, or is about to be transferred, across an EU border. Where PNR data is processed without crossing an EU border, it will be governed by the domestic data protection legislation of the relevant Member State; in the UK, this will be the Data Protection Act 1998. It is important to note that Member States gave an undertaking—which is written into the DPFD—that national data protection legislation would provide a standard of data protection which at least matched that provided by the DPFD, so there will be no gap in the level of data protection applied to PNR data processing. During the course of negotiations, many Member States, including the UK, have emphasised the importance of ensuring that adequate levels of data protection apply to PNR data. The Presidency has responded to these comments by drafting additional data protection articles.

We continue to engage the Information Commissioner's Office (ICO) closely on this matter; my officials discussed the Commission's proposal with both the Deputy and Assistant Information Commissioner only last week. As you will be aware, the ICO has been involved in discussions about our e-Borders programme from the earliest stages, has visited our passenger information unit and is reassured by our procedures.

Lisbon Treaty

I would also like to clarify the impact of the Lisbon Treaty on the EU PNR negotiations. When the Treaty comes into force next year, the draft PNR instrument will likely still be brought forward under a JHA legal base, but will be subject to Qualified Majority Voting and co-decision with the European Parliament. At this point, the UK would lose its power of veto but would have the choice over whether to opt-in to the measure or not.

Tom Dodd,
Director, Border and Visa Policy

7 April 2008

Further supplementary evidence by the Home Office

I understand that members of the Committee would appreciate some background information on Project Semaphore and e-Borders to be included as supplementary evidence in your forthcoming report on the draft EU PNR Framework Decision. I hope that the information below is helpful.

Project Semaphore

Between January 2005 and March 2008, the UK Government trialled the processing of passenger, service and crew data provided by carriers in order to support an intelligence-led approach to operating border controls. Project Semaphore was a pilot project aimed at testing an operational prototype in order to de-risk the development and delivery of the e-Borders solution. Semaphore initially targeted six million passenger movements a year, on a number of international air routes to and from the UK. After a successful first year and in the wake of 7 July 2005 London bombings, the project was granted additional funding to increase capability. From the initial single carrier and two routes, Semaphore grew to receive passenger data from 102

carriers and 182 arrival/departure points. Between January 2005 and March 2008, when the pilot concluded, Semaphore captured data on 47 million passenger movements and issued over 20,000 alerts to border agencies, resulting in more than 1,800 arrests and other interventions for crimes including murder, kidnap, rape, assault, firearms and fraud. These alerts and the data captured also made a significant contribution to countering terrorism.

Semaphore trialled the electronic processing of two main categories of data. The majority of passenger data captured was Advance Passenger Information (API) data which is also known as Travel Document Information (TDI). API contains biographical information from the passenger's travel document and the unique service information used by the carrier to identify each particular routing. API data is run against watch-lists in order to identify known individuals that pose a risk of harm to the UK and its citizens.

The second type of passenger information collected was Passenger Name Record (PNR) data. PNR is a term specific to scheduled air carriers and comprises reservation data collected by carriers for commercial purposes during the booking process and at check-in. The data cover up to 19 data fields including passenger name, travel itinerary, contact and billing information. PNR is alternatively referred to as Other Passenger Information (OPI) which can refer to booking information collected by other carriers including air, rail and maritime carriers. PNR data are used in two ways. Firstly, the data are checked electronically against carefully constructed profiles to identify passengers who appear to display high risk characteristics, but whose identifies are unknown to us. Secondly, we use PNR data to enrich ongoing investigations.

Under Project Semaphore we began processing PNR data on carefully selected routes from October 2005. The Government has never placed any obligation on carriers to collect specific PNR data indeed, we can only request such data as are known to the carrier. Usually fewer than half of the 19 data fields are collected by carriers.

e-Borders

On 1 March 2008 the package of legislation underpinning the e-Borders programme came into force. The legislation is formed of three statutory instruments: the Data Acquisition Order, the Duty to Share Order and the Code of Practice. e-Borders systems will provide the capability to risk assess all future passengers; and where necessary intervene against those considered to be high risk.

The UK Border Agency is required to balance its obligation to the security of the United Kingdom's border with that of facilitating the entry and exit of legitimate travellers. The e-Borders system will assist in maintaining that balance. The programme will provide an electronic record of people entering and leaving the UK through the collection of API data. By April 2009 e-Borders will handle data for 100 million international passenger and crew movements a year. The programme will be able to count 95% of all passengers in and out of the country by the end of 2010, with 100% coverage by March 2014.

PNR data will contribute to the passenger data collected. However, we will target the collection of PNR data on high-risk routes and aim to be collecting PNR on 100 million passenger movements a year by 2013. We will receive PNR data 24–48 hours before the scheduled departure time, API at check-in, a second supply of PNR data once the carrier is satisfied those data are final, and separate departure confirmation to confirm those passengers who are on board once the aircraft doors are sealed.

If you require any further information, please do not hesitate to contact me or my colleagues in Border and Visa Policy.

Tom Dodd
Director, Border and Visa Policy

6 May 2008

WEDNESDAY 2 APRIL 2008

Present
Dear, L.
Garden of Frognal., B
Henig, B.
Jopling, L. (Chairman)
Marlesford, L.
Mawson, L.
Teverson, L.

Ludford, B.

Examination of Witnesses

Witnesses: Ms Sophie in 't Veld, a Member of the European Parliament, Rapporteur of the LIBE Committee of the European Parliament for the draft PNR Framework Decision, and Ms Linda van Renssen, examined.

Q70 ***Chairman:*** Thank you very much for coming, it is extremely helpful, and also you have brought Linda van Renssen, who I understand is your assistant, is that right?
Ms in 't Veld: Yes.

Q71 ***Chairman:*** Welcome. We are on the record and you may have seen some of the questions which we are interested in asking you, so let me begin. As you know, we are doing a short inquiry into the Framework Decision on PNR and we would be most grateful to get your views and comments. The arrangements for the collection and transmission of PNR data are currently in place in the UK, France and Denmark, and other Member States we understand are likely to follow. Is it your view that this whole operation calls for a harmonised approach through EU legislation?
Ms in 't Veld: Yes and no. If there is going to be such a thing as an EU PNR scheme then I think it should be a real European scheme, not least because it is an incredible hassle for the carriers to have to deal with 27 different schemes. Besides, that was the whole reasoning behind the proposal, that there are certain countries which are doing this; therefore it would be better if we had something harmonised, but that is not actually what the Commission is proposing. However, before we ask this question I still think we need to ask the key question: is it actually necessary? That question still has not been answered and that is the question that we will keep asking in our discussions with the Commission and the Council. I refuse to get lured into a debate on the details when we have not answered that fundamental question.

Q72 ***Lord Teverson:*** Perhaps we could ask Sophie if she could briefly give us the Parliament's view on that broader issue before we get into these questions, and perhaps also how it views the possible transition into co-decision towards the end of the year.
Ms in 't Veld: As you know, the European Parliament was deeply unhappy with the EU/US agreement on the transfer of PNR. Unfortunately, the outcome of the court hearing was such that we basically sidelined ourselves, but I think that many of our fears and suspicions have proved to be true and, inversely, the usefulness of the system has not been proven. We have been asking consistently for evidence of the usefulness (or even the need) for the collection and use of PNR for the stated purpose, because everything always derives from the stated purpose, proportionality and the details of the arrangements. We have not received any evidence. The evidence that is trickling in seems to indicate that the targeted use of PNR, ie, not automated searches but when they are looking for something or someone specific, might be useful in particular for fighting crime, not even necessarily serious crime or organised crime but crime. Fine; we can argue about that, but the stated purpose is always the fight against terrorism and serious crime, so you can only measure the effectiveness against that and the effectiveness of the EU PNR agreement has not been demonstrated in any way. Furthermore, there was a first agreement back in 2004 that was annulled by the court. Then there was another one in 2006 to 2007, an interim one, and there was a final one which was concluded last year. It has not even been ratified yet. The ink on the agreement is not dry yet and the Americans are seeking bilateral arrangements with the Member States. It turns out that the single evaluation that took place, which was very superficial and where most of the work was done by the then Privacy Officer of the Department of Homeland Security, who was very good, seemed to indicate that they were not actually very strict in implementing the agreement. It is formulated in such a way that they can use the data for all sorts of purposes. They are not really bound to it. We have just been discussing it with Baroness Ludford. The legal status of the whole agreement is totally unclear. That is the kind of agreement that we are concluding. We have another agreement with Canada, which is a different one on a different legal basis, which has not been evaluated. We are going to negotiate one with Australia. South Korea started requiring the transfer of PNR data yesterday and there is no legal base, no agreement, no data protection, and the Commission and Council do not want to conclude an agreement. Why? It is a complete mystery to me. They will not answer. There

are even rumours that the Chinese might introduce the collection of PNR before the start of the Olympics. There is no strategy, no vision, and again there is no justification. You know that the European Parliament was extremely critical of it. The term that was used in the resolution that we adopted in July last year was that the agreement that was concluded with the US was "substantially flawed". That is very clear, I would say. Of course, we do not have a position yet on the proposals which are on the table now but the questions are essentially the same. As a matter of fact we have moved on since then. We have a bit more information on what we can and cannot expect, and I have to say that as far as I can judge across the political groups there is deep scepticism about all this. Also, you have to see it in the wider context. We tend to focus very much on what is right in front of us and that is the PNR proposals but, if you look at the wider context, let us start with anything to do with travel and passenger movements. We are talking about the collection of fingerprints, not one but ten. We are talking about an entry/exit system. We are talking about an electronic travel authorisation scheme, and for all modes of travel, not just air travel. People are beginning to look at train travel, boats, car. I do not know about the UK but in the Netherlands we are introducing a kind of congestion charge system which will register cars. We have a public transport system which will work with a chip card which will register your movements as well. Then, if you look at all the other sectors, it is not only about PNR because then you will say, "Oh, okay, if it is used for the right purposes ---", but there are telecommunications data, including the contents of our communications, postal data, medical data, bank data, credit card data, there are smart cameras, smart microphones, satellite surveillance, you name it. They are literally working on cameras which can look through walls, so basically they know everything about us. And then you go to back to PNR then and you ask yourself, "Is it actually going to make our lives safer?", because that is the stated purpose. I do not know. Frankly, I am getting the feeling that citizens are increasingly under surveillance and the right to hold the executive to account is being eroded rapidly. Maybe I should conclude on a more philosophical remark, which seems a bit exaggerated but still it makes me think. Everybody is looking at China now. The government of China, as we know, is obliging companies such as Google and Yahoo to submit their customer records to the authorities for national security purposes. We say, "That is outrageous. They are a dictatorship". Western governments are obliging Google and Yahoo to submit their customer records for national security purposes and we can no more hold our governments to account than the Chinese can. We still live in a democracy and I would like to keep it that way.

Q73 ***Lord Marlesford:*** Can I follow up your earlier point about the usefulness of PNR not yet being evaluated as far as we in Europe are concerned, and ask first of all whether the Commission are asking the United States Government (which presumably means the Department of Homeland Security) for an evaluation of the usefulness of PNR, and, secondly, whether the United States Government are indicating they are going to answer or whether they are being obstructive and saying it is too secret to answer or what? In other words, are you satisfied as the European Parliament that the Commission—presumably it is the Commission—is interrogating the US Government on the matters that you need to know about?
Ms in 't Veld: The Commission is not asking such questions. We have asked the Commission repeatedly to carry out the evaluation in such a manner, but there has only been one single evaluation since it entered into force in 2004, and that evaluation looked exclusively at the implementation of the agreement, in other words, were they indeed protecting our data as they had promised? The conclusion was no, or they had only started to implement it during the evaluation but they did not look at the usefulness. The report was not made public initially, and then it was but not the annexes, which contain the interesting bits, and the annexes gave the first indications of what the data are being used for, which was for all sorts of purposes, including, indeed, fighting small-time drug smugglers or other very valid purposes. I am not saying those are not valid purposes but the stated purpose was the fight against terrorism, and no, it is not evaluated against that stated purpose. All the information that we get we get from the other side of the ocean because the Americans are much better at holding their Government to account than we are, and they are asking much more critical questions about these things, so there are, let us say, internal reports.

Q74 ***Lord Marlesford:*** "They" meaning Congress?
Ms in 't Veld: The Americans. For example, there is something called the Government Accountability Office, which is a government agency which assesses policies and which is very good. Some of their reports are very alarming and if you read how effective—or, rather, ineffective—anti-terrorism measures are there will be ample reasons for asking very critical questions. Just yesterday I was reading a report that was done by the Inspector-General of the Department of Justice on how the FBI is managing the terrorist watch lists. It is a shambles, basically, and very sloppy. Those are not the terms that the Inspector-General uses but read the report. It is very interesting. That is the kind of information that we get. Then we got from this side of the ocean the report from your own Government on the use of PNR,

which basically says the same. It says, "It is very useful because we are catching all these criminals". That is very good; criminals should be behind bars, but that is not the stated purpose. Again, the stated purpose can be defined in terms of the subject: is it terrorism or the fight against crime or against infectious disease (which is another one which is now in the agreement with the US), or is it other things? Also, what is the kind of use they are making of the data? Is this for targeted, very concrete investigations into known suspects or known cases or groups of suspects? Are they actually looking for something or do they use the data for random, automated searches such as profiling and data mining? I always come back to purpose. If they say, "We need to violate your privacy for this particular purpose", then you can only measure the effectiveness against that. If they say, "We need these data in order to prevent terrorist attacks", they seem to suggest that by profiling and data mining they can prevent terrorist attacks. I am not a security expert but I have seen no evidence of that. For example, a couple of weeks ago we had somebody from the security of Schiphol Airport (which has its own security issues) and he said that PNR is useful for catching petty criminals and for very targeted specific searches. If you see someone and you think, "Hmm, there's something fishy here", then you may have access to their data, but that is a traditional method of investigation. Why would they need unlimited access to the whole database, data mining, profiling? For what outcome? Why do these data need to be stored for 13 years?

Q75 ***Chairman:*** We shall come to that. Before we get to it I think you talked about the UK Government and I think you were perhaps referring to a letter which was written to Mr Frattini by Meg Hillier. We will come to that in a moment, but, just going back a little, you made the point a second ago that Articles 1 and 11 limit the application of this proposal to combating terrorist offences and organised crime. Is it your view that it would be a mistake to use this information for wider law enforcement as well as immigration purposes, or do you think it ought to be confined, if it is to go ahead, to the business of terrorism and organised crime?
Ms in 't Veld: Let me make one thing clear for starters. Nobody in the European Parliament that I know is against the use of personal data for all sorts of security purposes, so using the data for those purposes in principle is okay, but it has to be clear from the very start what the data can and cannot be used for. The thing is that the proposal of Frattini very innocently says, "This is for the fight against terrorism and serious crime", which is already fairly broad, because we always think it is pretty obvious what that is, but it is not necessarily obvious. If you look, for example, at the definition of "serious crime" in Germany, it is very wide. It includes things that we would not consider to be serious crime. Terrorism as well: does that go as far as a terrorist act? It is using all sorts of different terms that might in some countries include, for example,—what do you call it, Sarah? Apologies—is that what you call it?

Q76 ***Baroness Ludford:*** We normally use "glorification of terrorism". It is very controversial, the definition of a terrorist act.
Ms in 't Veld: The thing is that if the data should be used for other purposes that should be said from the start, and if Frattini presents a proposal and says, "Don't you worry. We're not like the Bush Government. We will only use this for terrorism and serious crime". He really tried to reassure the Parliament, but fortunately minutes of secret meetings tend to fall off the photocopier. The first exchange of views that the representatives of the Member States had on the subject immediately opened up Pandora's box. They said, "We should retain the possibility of using it for all sorts of other purposes. We do not want to be limited to the defined storage periods. We do want to have access to sensitive data". There is also the matter of trust, I think. It is like the agreement with the Americans. I did not much like the substance of the agreement but, okay, at some point you can say we have at least agreed on something and they will stick to it and we can trust our allies or our governments to stick to it, but then every time you turn round they do something else. With governments too, if we are ever to adopt such a scheme and, to be perfectly honest, I am still not convinced that we should, the purpose has to be very clear from the start. Otherwise, if a citizen has a problem and wants to go to court, and he says, for example, "My personal data have been used for the wrong purpose", the purpose has to be clear; otherwise he does not have a case and governments will have complete freedom to arbitrarily use the data for all sorts of purposes.
Chairman: Let us talk about the UK experience.

Q77 ***Baroness Garden of Frognal:*** You have already alluded, I think, to the UK running Project Semaphore for three years, an e-Border system capturing PNR data. The data that they have captured on over 50 million passenger movements have generated over 21,000 alerts and contributed to over 1,700 arrests for serious crimes amongst others. I can pre-empt your reply, I think, but do you consider that this provides any justification for having more data captured than in the API system?
Ms in 't Veld: First of all, because I also read the report of the meeting you had with Ms Hillier and Mr Dodd and Mr Norris, I think we have to be very clear what we are talking about. I also met Ms Hillier two months ago, I think. There is still a lack of

understanding of what you can and cannot do with PNR. If we catch criminals, yes, that is of course a very valid purpose, but again it has to be very clear from the start what you can and cannot do with personal data. In a democracy citizens have rights and they have a right to know what the government can do to them and what the government cannot do, and unless the purpose is defined in great detail from the start you have no means by which to hold government to account or to complain or whatever. Ms Hillier said at some point when we met, "But it is very useful. On the basis of PNR we have identified a murderer", or a rapist or something, "and he is now behind bars". That is not possible. On the basis of PNR data you cannot identify a person. You identify a person on the basis of API data, and I see in the report of this meeting too that all the categories or data are mixed up. People are not clear about what they actually are. API data are the information contained in your passport and some basic travel information possibly. PNR data collected by the carriers for the purpose of organising travel you cannot use for identification. In many cases, incidentally, they do not even have this information; they only have the information that people have volunteered. I think in the agreement with the Americans we initially had a set of 34 different data which were then merged into 19 but they were still the same data, but on average a PNR file will only contain about ten of those data. For example, if you have no special requests, if you do not pay by credit card, that is all not contained in the file, so they will simply not have that information. It is simply not true that you can identify somebody on the basis of PNR. I do not know about this particular case that she gave me but it shows that they are catching people on the basis of other indications, and that is also what she said in the hearing. The thing is, they have information on somebody or on the actions or movements of groups of people and then they can use PNR data to support their case, but that is a traditional method of investigation. There is no need to set up a massive database of the data of all citizens; there is just no need. Even security people agree on that. I have spoken to public prosecutors in various countries who say the same thing. As somebody put it, "It makes our lives more difficult because if you are looking for a needle in a haystack the last thing you should do is make the haystack bigger". For a targeted search, where other sources of information are also used, that is one thing and that can be extremely useful in seeking out the bad guys, but this massive, indiscriminate collection and use of data of all people and using methods such as profiling and data mining, no.

Q78 ***Lord Dear:*** I would like to pick up on that last point. The only justification, it seems to me, for huge data banks is that you can then go in and mine or data-profile, because if you are not doing that you are just holding the material and not using it.
Ms in 't Veld: Exactly.

Q79 ***Lord Dear:*** Thank you for coming. I am sure that everyone agrees with me that your views are tremendously refreshing and not altogether unexpected, and I think I know the answer to the question I am going to pose to you anyway. It is really about motor transport and the difference between air transport and road transport and rail and maritime. There is a suggestion that the UK wants to extend the proposal to allow the collection of all modes of transport, maybe excluding road but perhaps you would comment on that as well. I wondered if you could reinforce the views, and I know you have given them already, that if you only leave it with aircraft and do not apply it to all the other modes of transport it would not be effective and would not be proportionate. You have covered that in generality already.
Ms in 't Veld: Again, I am not a technical expert but the proposal for an EU PNR applies only to the regular flights, not to charters, for example, so there are already exceptions built into the proposal. That means that there are already holes in this security measure (or they pretend it is), and yes, there are all these other modes of transport. You could even quite literally follow every single move of people by using satellite surveillance. Google Earth is available to everybody. It is not science fiction; it can be done, but then you really have to ask yourself: what is the purpose? Does it bring what we expect it to bring? That is always the question. I will never take any principle positions but we have to look at what it is that we want to achieve and whether this is the right instrument. I do not think this is the right instrument, for the reasons that you have just stated.

Q80 ***Lord Dear:*** Could I move on, because this is an allied point about Schengen and we all understand how that works, of course? There is another suggestion that the data should not only be across the Schengen borders into Schengen but movements between Schengen states and indeed even within an individual state. I guess I know what you are going to say but I have to pose the question to you: is this (a) a tenable position and (b) an achievable position, particularly inside an individual country, say, Belgium.
Ms in 't Veld: If governments decide that is what they want to do then it will happen, but fortunately public opinion is gradually waking up to these issues and asking the question, "Are we not giving up too much of our freedom for a purpose that is not clear?". I do not think it is going to come that far. I hope it is not going to come that far.

Q81 ***Lord Dear:*** Not as far as individual states?
Ms in 't Veld: No.

Q82 ***Lord Dear:*** But movement between Schengen states?
Ms in 't Veld: Yes.

Q83 ***Lord Dear:*** It would fly in the face of Schengen by doing that.
Ms in 't Veld: The thing is, with all the measures that we have taken, and again, when we are talking about the security measures, there is always somebody who will get up and say, "But we have to fight terrorists". First of all, the data which are being collected are being used for all sorts of purposes. For example, the Australians have a system whereby they use the data to screen people who want to adopt a child. They screen people on HIV. That has got nothing to do with terrorism. People have this illusion that the massive collection of data in itself is going to bring greater security, so public opinion has been very tolerant to governments and very often governments themselves do not understand very well how it works but they think the collection of data might come in handy at some point. I think a real smart terrorist will always find a hole. The holes in these schemes are so obvious from the very start, starting with the exceptions which are already created in the proposal on EU PNR. It reminds me of the other bit of legislation that was passed on data retention whereby, even before the legislation had been adopted, there were websites which explained to people how you could circumvent the measures. I really think we should at some point have the courage to take a step back and say, "Are we creating real security or fake security?". When we are talking about terrorism, yes, there are people out there who have very bad intentions and it only takes one, so if we take security measures they should be real security measures and not fake security measures.

Q84 ***Chairman:*** Let me get clear in my mind your attitude to all this and let me put it in a different context. In certain counties in the UK, maybe most counties, I do not know, the police on motorways or dual carriageways will put a van with a device that scans all number plates and a mile or two miles down the road they will have a car or somebody on a bike, and if a number plate comes past which denotes somebody that the police might be interested in, and I am talking about a national crime now, or if it is a stolen car, they will tell whoever it is down the road and they will stop and question whoever it is. Is it your view that that type of police surveillance is wrong and unduly intrusive?
Ms in 't Veld: It is interesting because in Germany they had a similar scheme which was just slammed down by the German Constitutional Court. There is a pilot scheme going on in the Netherlands. There is some debate about it in Parliament. I do not think people are terribly aware of it. If you ask me, yes, I think it is wrong. Why should you monitor every single person? If they have cameras taking pictures of people who are speeding and then at the end of the road they are pulled over and they have to pay their fines or their car is confiscated, fine, but why would you have surveillance of every single person on the road?

Q85 ***Chairman:*** But you have surveillance in terms of speeding with everybody who goes past a camera.
Ms in 't Veld: Yes, but then you pay your fine and that is it, but without a clear purpose ---? They have these campaigns where they go out and they are catching people who are speeding but that is a very clear purpose and it is a one-off.
Lord Dear: Could I ask another question?
Chairman: Lord Dear has a lifetime of experience in police work.

Q86 ***Lord Dear:*** The same system is in a good many police patrol cars. You do not have to put a camera by the side of the road. A lot of police patrol vehicles have got the cameras themselves because they drive down the motorway, the camera is looking at all the number plates and it will also tell whether the vehicle is insured or not, because now by law, as in most countries, you have to have the vehicle insured against third party risks, and you can tell immediately on a national database, because all the insurance companies now pull the information, whether that vehicle is insured or not, so you are checking everybody against a road traffic offence, which is insurance, serious but not a crime in the accepted sense. You are monitoring everyone for everything but you only stop those where you have pretty well 100% certainty that there is an offence committed. It is not random stopping which would have been the case before, "Can I see your licence?". You only stop the ones who you know pretty certainly have not got one or are involved in crime or it is a stolen car, so the certainty is only on the stop. I wonder if that jars with your philosophy.
Ms in 't Veld: Again, everything hinges on the purpose. If they set out to find people who have not paid their insurance --- incidentally, I think it is very important that the public are aware that these things are happening because very often they do not know. Another thing is that, when you are talking about databases, there is no database with 100% accuracy, because in the same pilot scheme that we had in the Netherlands, whereby all licence plates were photographed, there was a lady who got a speeding ticket or something, and she was very surprised when she got the bill at home because she said, "I was 150 kilometres away from that spot at that particular day

and I had my car with me". It turned out that somebody had fake licence plates, but in the end for her it was an incredible hassle to prove that she was not on the spot, and that is something which is creeping in. Whereas before the burden of proof was on the state or on the authorities to demonstrate that there was a very good reason to investigate somebody, now it is the other way round. People have to explain why they are not guilty. It has not come to the point where that is the situation in court but certainly when you are talking about PNR that is the situation. It is happening to me. Every time I go to the United States they take me out of the queue, I get a stamp on my boarding pass, I am entitled to secondary screening. They ask me all sorts of questions. Last time I was there I had my passport and something that looks like a passport but actually is not. It is some document that is provided by the European Parliament which looks fancy but is completely worthless. The guy was very suspicious, "What is this? Why do you have two passports?". I said, "It is not really a passport". "Well, it looks very suspicious to me. What is it?". I said, "It is from the European Parliament". "What's the European Parliament?". Why do I have to demonstrate that I am innocent? Of course, there is always a grey area because even before the time of electronic databases people would be taken out of the queue and pulled in for questioning simply on the basis of the personal assessment of the border guards.

Q87 ***Lord Marlesford:*** You have mentioned profiling in a rather adverse way. If you will agree a basic simplified premise that the object of all this stuff is to catch the bad guys and the subsidiary point is to cause minimum hassle to the good guys, that presumably must mean that you profile. If you take an easy example, the customs in any country, red channel, green channel, on the whole when they are looking at people in the green channel they are profiling in all sorts of ways—appearance and all the rest of it—as to who they will pull out and look at. Are you opposed to profiling as a concept or just some ways in which it is used? What is your worry about profiling?
Ms in 't Veld: First of all, it is not very effective. As I said, there is always a degree of profiling even just in the head of the border guards. They have their instincts and they will look at you and say, "Hmm", but it is not very effective. Again, this is not something that I invent. All this information can be found in the Department of Homeland Security, for example, which I think is a reliable source. They do an annual report on profiling and Congress had a session about it. What they do is they use the same method as marketeers. They say if you are driving a Volvo and you spend your summer holidays with ClubMed then you are also very likely to have dinner at so-and-so restaurant. If they have, say, a 5% match they are happy, but that is not good enough for security purposes. If you look at the effectiveness of the terrorist watch list, for example, there are, I think, close to a million people on the US terrorist watch list. Those people are not all potential terrorists. As a matter of fact, most of them are not. There are many mistakes, there are many duplications. I just referred to this report by the Department of Justice on how the FBI is managing these watch lists. There are so many mistakes that they are just not reliable. Again, the Government Accountability Office found that the customs and border protection is so busy screening those people on the watch list that real wanted criminals manage to get into the country unseen. As an instrument it is not precise enough. It is just not good enough.

Q88 ***Lord Mawson:*** Do you know whether the profiling of passengers under the Framework Decision would raise constitutional concerns in any Member States?
Ms in 't Veld: I know that there are constitutional objections in Germany but I think that is more to do with things like storage periods and purpose than profiling itself, although it may well be that it is also the profiling. I do not know about other countries.

Q89 ***Lord Mawson:*** The UK believes that sensitive personal data are useful and would like the processing of sensitive personal data to be allowed under the Framework Decision, subject to specific data protection safeguards. What is your view? What safeguards do you think would be needed?
Ms in 't Veld: There are hardly any safeguards at the moment. Again, if you are looking for, let us say, a known suspect; you have a concrete investigation. If you follow all the right procedures or you have a court order or whatever, as policemen, for example, you have to demonstrate that there is reason to believe that this person has done something. Okay; then you have a reason for investigation and in that case, yes, the authorities should get access to information and if necessary also to sensitive information. Should these data be collected systematically? No. That is the other thing. Any security measure that we take has to be accompanied by a strengthening of citizens' rights. In the hearing you had with Minister Hillier she says that there is a data protection framework in place. There is not. The Council is trying to agree on a framework for data protection but it has not yet agreed one and it is a very bad arrangement. It has been criticised heavily by the data protection authorities. There are some Member States which are not happy with it. The European Parliament is not happy with it. I will give you a very clear example of why it is flawed, and it is precisely on the use of sensitive data. There is a paragraph saying,

"The use of sensitive data is not allowed—only in exceptional circumstances". Who decides? Who monitors? What exceptional circumstances? That goes to the whole Framework Decision on data protection in the Third Pillar. It leaves it completely open, so instead of strengthening the legal protection of citizens it has weakened it and it gives far too much discretion to the authorities. If we say a certain category of data can be used for certain purposes, then at the same time citizens have to be protected against abuse and mistakes and leaking by the authorities.

Q90 ***Lord Teverson:*** I think in a way you have just answered my question. What I am very interested to understand is, who is the champion of this? Is it Frattini? Is it the Commission that wanted this in the first place or is it particular Member States, in your view?
Ms in 't Veld: A bit of everything really. Frattini himself is very keen on this and even if the Commission put forward a proposal as the college I do not think any of his colleagues are really looking into the details. Of course, there are certain Member States who are pushing for this, not least the UK, and the reasoning that was given to us was, "Certain Member States are using this anyway, so it is better if we have it for the whole of Europe".

Q91 ***Lord Teverson:*** What Member States other than the UK are particularly interested in this proposal?
Ms in 't Veld: I get the impression that in this case it is mainly the UK and France, although even within Member States it may differ. For example, the German Minister for the Interior, Mr Schäuble, is very keen on any security measure, whereas his colleague at the Ministry of Justice fundamentally disagrees.

Q92 ***Chairman:*** Is that a function of the coalition in Germany?
Ms in 't Veld: I think Schäuble personally is very much a hawk, if you want, but Germany as a whole has a very strong tradition of civil rights.

Q93 ***Chairman:*** You could have fooled me!
Ms in 't Veld: Okay, since the Second World War. Let me rephrase that: they have a very good reason for being very critical when it comes to these things, and, interestingly, so do the United States. They take many measures which have a kind of extraterritorial impact, which would never be accepted by their own citizens.

Q94 ***Lord Teverson:*** You mentioned yourself that increasing numbers of third countries are likely to request the provision of PNR and I personally was not aware of that. We are interested in where you think that will go in terms of global collection and processing of PNR. Where is all this going to go? I presume in some ways the EU is quite pivotal to what might happen there. Is there a possibility, because it has been championed by an individual or only one or two states, that it might not get anywhere, or is this going to happen?
Ms in 't Veld: I am an optimist, so --- In a way the standard has already been set by the US. They have simply imposed it on us and push and push and push, because if you look at what they were asking for in 2003 and where we are now there is already considerable widening of the scope. Yes, the EU is pivotal and, of course, if you look at an organisation such as ICAO, for example, they are trying to come up with proposals for a global standard because they want to have influence but they are also a bit worried about the course that this is all taking.

Q95 ***Lord Teverson:*** You are in a way saying that this is probably good if we are very clear what it is for and we only use it for what it is for, and if it is effective to do what we say it is going to do.
Ms in 't Veld: Yes, and with the legal safeguards in place.

Q96 ***Lord Teverson:*** Yes. What I would be very interested to understand from you is, from your point of view within open societies how do we determine whether this is effective or not? I do not want to get too much back into the American system, but is it possible to show that it is effective or not from the point of view of parliamentary scrutiny, whether it be national or European?
Ms in 't Veld: Let me put it this way. If the people who are proposing this are so convinced that it is useful then I am sure they have all the supporting evidence, I would say, in my limited logic. It is just that they have never produced it and every time you get the same argument, "Oh, no, we cannot tell you that for security purposes".

Q97 ***Lord Teverson:*** Is that a valid argument? Can that be an valid argument?
Ms in 't Veld: It is not a valid argument. It is never a valid argument in a democracy. In a democracy if the executive cannot be held to account then we have a serious problem. Of course, you do not have to print it in the newspaper but there are all sorts of mechanisms in any democratic state for controlling the government and even in sensitive security matters. All we have asked for, for example, is facts and figures which would not give away any operational details, "How many bad guys did you catch, how many attacks were prevented and how many false positives were there?". That they should be able to answer without giving away details. We

could even accept that they would do it in a closed meeting, but all you get are horror stories by Mr Chertoff which impress his audience, but, sorry, we are legislators. If I put my stamp of approval as a Member of Parliament on the law then I want to be absolutely sure that it has a solid justification, and we just never get any proper evidence. Mr Frattini says, "I believe that it is necessary". If the Government proposes to spend 20 million on infrastructure works, would you say, "I accept it as a Member of Parliament" if they say, "We believe it is useful"?

Q98 ***Lord Teverson:*** Well, they did build the Dome in East London, so I am afraid we failed.
Ms in 't Veld: The other thing is that we all seem to believe that these systems are infallible. We seem to have blind faith both in government and in technology, which is rubbish. For example, ask Symantec, which is a company which makes security protection systems for computers, for the figures on how that security works in practice. The worst offenders, when it comes to leaking personal data from databases, are public authorities and the education sector is the worst with 30% of their databases. On average it was 25% but I have heard that it is just going up. We all know the stories. I think you had your CD Roms and we had our USB sticks there in all these companies or sites of public authorities which all of a sudden turn out to be accessible to everybody or can be hacked. There is no 100% security. As a matter of fact they are very sloppy, so that would be another thing where I would need better guarantees.
Chairman: I think you have made it very clear what your personal attitude toward this is but let us just now turn to the wider aspect of the politics of the Parliament as a whole.
Baroness Henig: Obviously, if the Treaty of Lisbon were in force at this point in time this measure would need co-decision and I wondered what steps the Council has thus far taken to involve the European Parliament more closely, because it is likely that as and when serious moves are made on this there will be a system of co-decision in place.

Q99 ***Chairman:*** As well as, if I might say, your assessment of how the Parliament will respond to these proposals. You have made your personal position very clear.
Ms in 't Veld: To start with the last question, of course people will express their views. There is a wide range of different tones of voice but all in all, as I just told you, the resolution that has been passed by the European Parliament last year on the EU/US agreement is crystal clear and this was supported with near unanimity in the European Parliament. So far we have not started to work on the text of the EU proposals but what I hear from all the political groups so far is that they all share the same scepticism, the same doubts; they all have the same questions. The spokesperson of the EPP group, which is the Conservative Christian Democrat Group, which always tends to be a bit more law-and-order, is saying the same thing. They say, "We want evidence first and we are not getting it". The more the Commission is refusing to give it the more they dig their heels in. I do not know if you share this assessment.

Q100 ***Baroness Ludford:*** Yes.
Ms in 't Veld: This is the position so far. We do not know where it will go.

Q101 ***Baroness Ludford:*** I am not sure what the whole EPP position will be. The Spanish party tends to be pretty hard-line, and some of the Germans.
Ms in 't Veld: Okay, but the spokesperson of the EPP is a German. That is one question. The other question was, what has the Council done so far? Nothing. Here is a little anecdote. When we were talking about the EU/US agreement last year—this was under the Finnish Presidency—the Finnish Minister for Justice, I believe, came to our committee and reported on the PNR file, and she said, "And we have been in close contact with the rapporteur", which was me. I thought, "I have never seen this woman before in my life". They have done nothing. At an informal level we have pretty good contacts with the Commission but, no, we do not get information, as I said, other than through the grapevine. The funny thing is, of course, that one way or another we will get co-decision because if it is carried over into 2009, and it is very likely that it will be because there does not seem to be a great deal of consensus within the Council, then it will be co-decision in any case. The Legal Service of the Council itself has argued that the current legal base is the wrong one, that it should have a kind of double base for two parts of the proposal and one part should be on the basis of transport policies, which is then also co-decision. One way or another we will get co-decision but they do not seem to be fully aware of that yet.

Q102 ***Baroness Henig:*** It sounds therefore as if there are going to be interesting times ahead.
Ms in 't Veld: Yes.

Q103 ***Baroness Henig:*** Maybe even quite stormy times ahead.
Ms in 't Veld: Yes. At the start I mentioned how many categories of data there were. Basically, any database is accessible by government agencies these days, but this particular one, even if it is only one small subject, has become very much a symbol of the whole debate.

Q104 ***Baroness Ludford:*** I would say: with the exception of the UK Government, which in the person of Meg Hillier is indeed on a charm offensive, which to me is rather reminiscent of the Home Secretary at the time, Charles Clarke, under the UK Presidency in the second half of 2005 on the Data Retention Directive.
Ms in 't Veld: That is true, but there have been these work sessions with representatives of the Member States and we said, "Why do you not invite us, maybe the rapporteur, maybe the representatives of the other political groups? As they are work sessions anyway it does not matter". "Ah, no, no, we never do that". Okay.

Q105 ***Lord Marlesford:*** My question follows on neatly from that because I gather your committee is visiting England to see the Joint Border Operations Centre near Heathrow.
Ms in 't Veld: Yes, it so seems.

Q106 ***Lord Marlesford:*** What do you expect to get out of that? When are you going?
Ms in 't Veld: We have no idea. I read about it in this report yesterday. I do not know, but I am very keen on going. In our committee we had the guy I referred to earlier from Schiphol security who gave us a bit of background on how these things work in practice, and I imagine what we will see, or what I hope we will see, is indeed how they use the data.

Q107 ***Lord Marlesford:*** But there has not been a joined-up invitation yet. It has come via us, has it?
Ms in 't Veld: Yes. When we met with Ms Hillier we said, "Oh, yes, that would be a really good idea", but there has not been a formal invitation. I am sure that everybody will be very happy to go.
Baroness Ludford: I met the Director of European and International Affairs, Christophe Prince, at the Border and Immigration Agency, who was in my office this morning and he said that and I said, "Yes, when we have the invitation", and he took on board the fact that we had not actually had an invitation.

Q108 ***Chairman:*** We got an invitation direct from the horse's mouth, as it were. I call it that politely. She is, incidentally, an extremely impressive lady, we thought.
Ms in 't Veld: And very nice too.

Q109 ***Chairman:*** Yes. They do not always go together but we were very impressed with her. I wonder if any of my colleagues have any other questions they would like to ask as a follow-up to this. No? Sophie, is there anything more you would like to add?
Ms in 't Veld: Yes, there are three small points that I would like to add. One is on the API that I mentioned earlier, which is the basic information which is used for identifying people. There is a European directive on that as well which has been implemented so far by five Member States, or there may be six by today, but the implementation rate is very low. You would think that if it is all so urgent for security purposes they would make bigger haste with this. Secondly, again on the effectiveness, I would like to remind everybody that in all the high profile cases of terrorist attacks the information necessary was available. Just last week there was a report on how the Dutch Intelligence Service had handled the case of the murder of Theo van Gogh. It turned out that they had everything they needed. They could have prevented it and they did not because their risk analysis was wrong because they did not share information because of bureaucratic cock-ups—because, because, because. Take 9/11—they were already watching these people. Madrid—they had the information on who these individuals were but it turned out that the countries were not exchanging information, so it is not as if the problem has always been that there was insufficient information or that they did not have sufficient powers. It is also how you use those powers and that brings me back to the report on the terrorist watch list and the way the FBI manages it. Those are really key issues and it is not about criticising the FBI, but if we are collecting personal data of people and saying that they will be used for greater security but then we see that our agencies are still not working together, still not exchanging information, then the accuracy of data and watch lists leaves room for improvement, let me put it that way. Those questions are also key.

Q110 ***Lord Mawson:*** I have spent many years on a housing estate and one watched these endless systems passing through, which were massively ineffective, and generally I found that when you wanted information it was about talking to one or two of the right people whom you got to know as people. One wonders whether with many of these large systems part of the problem is that people are relying on systems, processes and structures rather than trusting people and relationships and so you end up in these sorts of difficulties.
Ms in 't Veld: Yes. The trend is that government agencies or public authorities do not set up new databases. What they do is get access to databases which have been created for commercial purposes, whether it is airline companies or Google or your insurance company or your telecoms provider or your internet provider, you name it. Of course, they do not create databases for the purposes of law enforcement and security, so for them the accuracy of certain data is not particularly relevant. Many mistakes are made when the data are fed into the

system. For example, when we were talking about the Data Retention Directive somebody from a telecoms provider said, "All we need are the data of a person to be able to send that person a bill", so whether his or her name is actually the name in his or her passport, whether the street address is the right one, they do not really care as long as they can find the person and they pay the bill. Many people will get a telephone subscription, for example, and give an email address or a credit card number or whatever. Two years down the road they have changed their email address and they have got a different credit card but they have never bothered to change the information because it was not relevant, so all these databases are not terribly reliable.

Q111 ***Lord Dear:*** Just as a matter of interest, all our terrorists were home-grown and born and bred third generation in our own country. They may never have moved out.
Ms in 't Veld: Exactly.

Q112 ***Lord Dear:*** So looking at travel for them was pretty fruitless.
Ms in 't Veld: Yes, and terrorists these days are very smart. Well, fortunately, they are not that smart. I have been doing a bit of reading on failed and prevented terrorist attacks and in many cases they are incredibly stupid, fortunately, but, as I have said, it only takes one who succeeds, and they are finding their way around things. For example, they will meet in a place far away from the city where their telephones cannot be traced because there is no network. They are probably not going to travel by plane. They are not going to send their money via international bank transfer. They will make their phone calls from a phone booth. Okay, you do not go completely undetected but you can stay below the radar. I have one last point, which is a bit of a technicality, going back to data protection. The data protection systems that we have are completely inadequate, never mind the fact that the Framework Decision has not been adopted yet, but there is another interesting thing. If you look at these minutes (which we are not supposed to have) of the meeting in early February on the first working session and exchange of views between the Member States' representatives, it is interesting what they say about data protection. They say, "There is a small problem because the current Data Protection Directive", which applies to the First Pillar, ie, to businesses, "would cover the collection of PNR data by the carriers". If and when the Framework Decision on data protection in the Third Pillar is adopted that would cover the use and exchange between Member States of those personal data. However, the transfer of data from the carriers to the government agencies is not covered by any data protection arrangement, and it says in the minutes, "but we will find ad hoc solutions to that". If you listen to Frattini and all the other advocates of these measures they always say, "But we need to find the right balance between security and privacy". It is a non-statement; it is completely meaningless. If you then look at what they say to each other when they believe nobody is watching it is very frightening, I think.
Baroness Ludford: I think you are going to meet Peter Hustinx, who is the European Data Protection Supervisor. He said something I thought was very interesting. He said that the normal rule of law—I am paraphrasing his opinion on this proposal from memory—is that you apply criminal justice to someone on the basis of that person's own behaviour, whereas the essence of these data collection systems which are going to partly be used for profiling and data mining is that you are doing something to someone on the basis of other people's behaviour because the behavioural profile that you are then going to apply to pick people out is based on other people's behaviour. It is slightly philosophical; I was not sure it was a legal point, but you are undermining the rule of law, which is that only a person's own behaviour gets them in trouble. Also, in the Framework Decision proposal itself, again from memory, I think it says that PNR data cannot be the basis for enforcement action. I would invite you if I may to try and test what "enforcement action" means. If it is used for secondary screening, if it is going to become a flag in a database on someone, is that enforcement action? What exactly do the terms mean? You do get big legal problems about what happens to people on the basis of being picked out as a result of profiling and then what happens to them compared to, if you like, the strict rule of law.
Chairman: It has just been pointed out to me that the document does say that passenger information units and the competent authorities "shall not take any enforcement action solely on the basis of automated processing of PNR data".

Q113 ***Baroness Ludford:*** Again, what does "solely" mean?
Ms in 't Veld: In this respect I was quite shocked to read in the report of your meeting with Ms Hillier, " . . . we have arrested and prosecuted drug traffickers on the basis of their travel patterns and their travel history, not on the fact that their name has appeared on our watch list . . . ". I think, again, that if you decide to introduce systems like this there need to be watertight legal safeguards for civil rights and there are not.

Q114 ***Chairman:*** We are most grateful. We have gone through all our questions. You have given us very full answers. You have applied your personal opinions liberally into them, for which we are

particularly grateful and which is why we wanted to talk to you, and this will help us enormously in producing a report which we shall be agreeing by the end of this month and producing it, hopefully, by the end of May.

Ms in 't Veld: I am looking forward to it.

Q115 ***Chairman:*** Thank you very much for coming.
Ms in 't Veld: Thank you for the invitation.

WEDNESDAY 2 APRIL 2008

Present
Dear, L.
Garden of Frognal, B.
Henig, B.
Jopling, L. (Chairman)
Marlesford, L.
Mawson, L.
Teverson, L.

Examination of Witnesses

Witnesses: Ms Cecilia Verkleij, Head of Sector, and Ms Despina Vassiliadou, European Commission, examined.

Q116 ***Chairman:*** Cecilia Verkleij, thank you very much indeed for coming. I think you have appeared previously before this Committee.
Ms Verkleij: Yes.

Q117 ***Chairman:*** I think you came with Jonathan Faull. I was not able to be at that meeting, which was some time ago, but you have brought with you today Despina Vassiliadou. Thank you very much also for coming. We are on the record. As you may know, this Committee is doing an extremely brief inquiry into the latest developments on a European version of PNR and we had a very forthright evidence session before lunch with Sophie in't Veld, whom you no doubt know well, and you probably will be aware of many of the things she has said about the whole business of records and the attitude of the Commission. She has told us what she thinks might be the attitude of the Parliament but we will discuss those things in greater depth over the next hour. If you look at Article 1 and Article 11 of the Framework Decision, they speak of limiting the processing of data to combating terrorist offences and organised crime. What would be the attitude of the Commission to the use of PNR to combat illegal activities beyond those two fears? I do realise that there may be differences as to how you interpret those two definitions, but if you could begin by talking about that we would be grateful.
Ms Verkleij: Thank you for inviting us to come and join you today to explain the Commission's point of view on this proposal, albeit we are at the early stages of the discussion in Council, but already a few things can be said on how the discussions are developing so we think it is a very timely moment to discuss these issues with you. On your question, it is true: Article 1 provides us with a purpose limitation, and a purpose limitation is an issue which is of huge importance, both for law enforcement and for data protection. It provides law enforcement with a clear idea for which purposes to use the data but also for which purposes not to use the data, and from a privacy point of view it is very important because it responds to the criteria of necessity and proportionality. Both security and privacy benefit from a purpose limitation. It is the Commission's view that a purpose limitation should be a purpose limitation, meaning that you should look at very specific purposes for which you use the data, and that is why we have proposed in our proposal to look at terrorism and organised crime. Why? Because we have different Community or European Union instruments where you may find definitions of these offences and crimes, so we try to link into already existing policy. When we contemplated the scope of Article 1 we also had to bear in mind differences of view between Member States. We are for the time being still in the Third Pillar, as we call it, and therefore we had to bear in mind that we needed unanimity at some point in time, so we tried to balance in our project the different strands of the Member States.
Chairman: In reply to the question you used the word "should" rather than "must". I think that takes us straight into questions that Lady Garden may like to ask, particularly so far as the UK is concerned.

Q118 ***Baroness Garden of Frognal:*** The UK Government has also suggested that PNR might be used for immigration and revenue and customs purposes. Would the Commission have any objection to that, and since these are First Pillar matters how could the legal difficulties be resolved?
Ms Verkleij: As I explained earlier, for the time being under the current treaties we are obliged to stay within the limits which those treaties impose upon us, which means you cannot regulate in a Third Pillar instrument matters that are under the First Pillar. That would amount to contravening Article 47 of the treaty, so that would be illegal. We had to limit the proposal to police and judicial co-operation and in this instance it is police co-operation. That is why we could not even contemplate looking at purposes that might serve for First Pillar purposes. However, if we look to the future and to Lisbon, Lisbon will do away with those two Pillars and we think that the proposal will not be finalised before Lisbon enters into force (the presumption being that Lisbon will enter into force by the end of this year), and that means that we will then have to review the situation. Taking that as our starting point, we have had some reflection

internally but also during the discussions with Member States, and Despina can take you through those discussions. It is one thing to ask do we want to use the PNR for immigration, revenue and customs purposes as such. We would have great difficulty in using the data for those purposes without any limitation. We are not convinced that PNR data are really made for servicing those purposes but we also have to bear in mind the issue of proportionality, and again we have to bear in mind the different positions of Member States. Perhaps Despina would like to fill in on that part.

Ms Vassiliadou: The discussions in the Council for the time being show that a large majority of Member States are in favour of extending the purpose limitation of this proposal to cover serious crime as well. To the extent that immigration, revenue and customs offences are not immigration, revenue and customs policy in general, the offences could be covered by such a definition of serious crime, and to that extent the discussions are still ongoing in Council and we cannot predict how things will develop for the time being but we can see that other Member States share to some extent the views of the United Kingdom Government as expressed in the discussions, but they would like to see a wider purpose limitation to cover serious crime as well.

Ms Verkleij: That would mean that we could contemplate within Council, according to how the discussions develop, an extension of the scope to cover serious crimes to the extent that they are not already covered by "organised crime" and we can get guidance from European Union instruments, in particular the European arrest warrant. In Article 2.2 of the Framework Decision on the European Arrest Warrant there is a list of serious crimes which we very often use in the discussions with Member States, and you will find that one of the serious crimes listed in that article is what is called "facilitation of unauthorised entry and residence". That looks like an immigration issue but to us that would not mean that the scope of the instrument would be widened to immigration purposes as such. If it was part of serious crime, and if all the Member States agreed on that, that would be a way to accommodate different concerns and in particular the UK concern that we may be faced with serious crimes which are not necessarily organised crimes but where you would like to identify certain travellers and make sure that you can prosecute them if they have committed a serious crime. The discussions in Council are going in that direction but, as I said earlier, a purpose limitation should be a purpose limitation, so the scope should be defined as precisely as possible.

Q119 ***Baroness Garden of Frognal:*** Could I specifically ask you about the letter from our Home Office Minister to Vice-President Frattini about Project Semaphore? Do you think that the arguments in the Minister's letter justify the use of PNR for wider purposes? You have partly answered that already but perhaps you could answer that specifically.

Ms Verkleij: We are very happy in general with the way the UK and its ministers inform us about their projects because it allows to feed that into the wider European debate and we are very happy also that they have already accommodated a lot of visits, including by ourselves. We had the opportunity to visit Semaphore twice, once last year and also towards the end of the pilot project, and that has been very important for our thinking and also in further developing our thinking because this project is the only one in Europe which is up and running and can show you tangible results. It was great to see that and to get all the explanations from those who are in the lead on that project. Your Minister's letter is part of that exercise and it was very much welcomed by Vice-President Frattini. It was seen as support for our policy which was extremely welcome and which we felt was something we needed also in the discussions leading up to the informal JAI Council in January where ministers indeed decided that we should go ahead with this project. In the letter the Minister refers to successes which have been obtained by your services as a result of the data. These are, of course, general references. I think the letter mentions a number of successes, which are important but at the same time I think it also triggers again the question on which set of data these successes have been based. Are these PNR or API data? There is a distinction to be made there and that distinction in our view also links into the question, "Do you want to use the data for immigration purposes?". We have had that as the basis of our proposal, what kind of information we are looking at and how this information can be used for preventing and fighting certain types of crime, with the idea in our minds that law enforcement perhaps does not need a large amount of data but the appropriate set of data, the right set of data, and the great advantage of PNR and API data is that they are different from each other, and they also serve complementary purposes. Of course, it is not the purpose of a letter to set out in detail these sorts of things. What we appreciated very much was the fact that there was clear support for our proposal ahead of the ministers' meeting and the successes mentioned showed us that there was a case for using these data, that it is not just something we have invented but that there is an actual law enforcement need, and that that need can also be accommodated by providing the necessary privacy rules. In general we are very happy with the letter. We are not at this point in time fully convinced that this set of data can serve all the purposes which the Minister may have in mind. On the other hand it may be an issue of defining a bit

more precisely which data serve which purposes, and API data are the data which you ideally would use for immigration purposes, so I do not exclude that we may be talking about the same thing after all at the end of the day.

Q120 ***Chairman:*** Can I just follow those answers up a little bit? You sounded to me as though you were giving a green light to Meg Hillier's letter to the Vice-President in that she was sympathetic to it, and you said earlier that the limitation which had been put into Article 1 of the Framework Decision was recognising the differences of opinion. Does that mean that you think you could get a better deal and a better result once the Lisbon Treaty is in effect rather than trying to drive it through between now and the end of the year, say, whereas you might then have the advantage of not having to go to co-decision? I can see that there are quite difficult tactical decisions to take here by the Commission. Do you leave it until next year where you can get a broader and more satisfactory outcome, or do you drive it through so that you can try and do it without having to achieve co-decision with the Parliament? Is that a fair assessment of the tactical options that face you?
Ms Verkleij: There are practical and tactical options which face us, the first one being that in the current situation we do not think it is feasible to rush 27 Member States into this proposal without thinking it through in all its detail. This proposal is quite challenging for the Member States in the sense that it should work operationally. It is very nice to have a proposal which on paper looks like you are providing the right set of data to law enforcement, but if it does not work operationally then we have done the wrong job. One of the issues on the table which has not been discussed yet, because we are only in the first reading, is, how the different law enforcement authorities in the different Member States will exchange information, which information they will exchange and how they will do that. Do we need a central database for this or do we need decentralised databases? These questions can only be answered when you know what kind of purpose the data can serve, and that debate is not finalised yet. My impression is, but, Despina, please tell me if I am wrong, that this may still need some time. We are not afraid of co-decision so we are not rushing anything through because as from 1 January we will have to face the Parliament. On the contrary, we love to have this debate also with the Parliament because, as you yourself already assume, it looks like Lisbon will give us a better deal. If that gives us a better deal why should we rush into something which in our view, and talking also to the operational people in Member States, would probably cause at the end of the day many more problems at the level of implementation because of having it rushed through. What we have already tried to anticipate are possible problems at operational level because it is one thing to legislate; it is another thing to get it implemented in 27 Member States. I do hope that answers your question.

Q121 ***Chairman:*** You say you are not afraid of the Parliament.
Ms Verkleij: Oh, no, not at all.
Chairman: If you had been here this morning, from what we heard you would have every reasons to be worried about the Parliament!

Q122 ***Lord Teverson:*** I wanted to follow up something you mentioned from Lord Jopling's question. One of the things I do not fundamentally understand here is who does all this data belong to? Does it belong to the Commission, does it belong to individual Member States that have collected it or does it remain with the airline companies? Also, what is envisaged? Is it one big database or is it 27 different ones, and who develops this and who pays for this and who manages this? Of course, when you get to that point you think, well, the legislative process, even if it was a hostile Parliament, would be the easy bit in comparison with the systems development. This Committee, as you know, has looked at Schengen II and Schengen one-for-all and all of those, and the time span tends to be such that maybe we will be in the next Reform Treaty before we have finished this database. I would be interested in your views.
Ms Verkleij: You can have as many Reform Treaties as you want. We can accommodate that.

Q123 ***Lord Teverson:*** We are promised this is the last.
Ms Verkleij: I see your point and that is exactly why we think nobody is for rushing this project through by the end of the year. That is not our aim in view of Lisbon. Your question is right. Who owns the data? For the time being, certainly not the Commission. There is no system up and running which is being managed by the Commission and we do not propose that in the proposal either. What we suggest are decentralised databases, which means that the data are owned by the air carriers as from the moment they receive the data from the passenger, so from the moment booking starts up till the moment that the data are transferred, either directly to the authorities of the Member States or via an intermediary. From the moment they are received by the authorities of the Member State the Member State will then become responsible for those data under law enforcement data protection provisions. That is how it will work. One of the issues on the table is, do we provide for a system which is a kind of one-stop shop where an air carrier entering the European territory would send the data to one address, or do we want the air carrier

to send the data from a flight from Washington to Paris to the French authorities and from a flight from Washington to Barcelona to the Spanish authorities, and so on? Again, that is a discussion which we will probably only enter into once we have a much better view of what the purpose will be, because the purpose is defined also as how you are going to use the data for the needs of law enforcement. That has not been discussed fully yet and my impression is that it will be one of the most difficult issues to tackle.

Q124 ***Lord Mawson:*** Could you summarise the position of Member States on the scope of the Framework Decision and do you believe that extending the permitted purposes through the domestic legislation will give rise to questions over the principle of loyal co-operation? Would it give rise to other legal inconsistencies?
Ms Verkleij: I will leave the first part of your question to Despina who is in the lead in Council on discussing this with Member States.
Ms Vassiliadou: The discussions in Council have indicated that the majority of the Member States would prefer to have a wider purpose and they are talking about substituting "organised crime" with "serious crime" which would cover a larger majority of offences. That being said, I have to note that all Member States for the time being have scrutiny reservations, so one cannot take these initial positions as their final positions.
Ms Verkleij: As I said earlier, we are only at the first reading and we notice that quite a few Member States have made a general scrutiny reservation and are also waiting to get clear instructions from their capitals on some of the issues, including the permitted purposes, but there is certainly a willingness both by Member States and the Commission to dig into that issue because it is essential to what the system at the end of the day can deliver. We are very grateful to the UK for being so involved in that thinking from the beginning. Suppose that we could not accommodate all the UK wishes for this particular proposal, would we then not mind the UK going further domestically? I think we would. I think we would not be very happy if domestically the scope were wider. One has to bear in mind that one of the aims of this proposal is not only to identify and bar high risk passengers from entry into your country, but also to share some information about these people. Sharing information always has the component of trust, that the data you share do not end up somewhere where you do not want them to end up. If we all have the same purpose and if we all have the same set of guarantees that should work. At least you do not have an excuse to say the data I send you may be used for a different purpose or may end up in a database I do not want it to end up in, but if you allow a Member State to go further domestically this will be in the mind of the other Member States who need to share the data amongst themselves and, as I said, we have to bear in mind that this is a project for 27 Member States who may not always necessarily share the same opinion among themselves, particularly on the purpose. For that particular reason we would very much be in favour of ensuring that all Member States could agree on the purpose limitation, which would be a guarantee that would build trust once this system became operational and once they started sharing the data amongst themselves.

Q125 ***Lord Mawson:*** Can I ask you another question about this? Often in my experience politicians have all sorts of aspirations about what they would like to happen in the world, but we know from experience in Britain and elsewhere in using IT systems and data systems the realities of what they can and cannot do and how that works in practice can sometimes be altogether different. Who is advising you on the technicalities of what is possible and what is not possible and how it might work in practice, because sometimes the gulf there can be immense?
Ms Verkleij: Thank you for asking that question. We launched last year a request for a study on this issue in particular because we needed guidance not only on the question of the effectiveness of centralised versus decentralised databases but also on what IT can do and what it cannot do. From the operational point of view, so for law enforcement, and also for privacy implications, what can IT do to enhance privacy? Despina was the author of that project.
Ms Vassiliadou: As my colleague explained, we have launched a tender for a study on how technology can help and what it can and cannot do in this field. We have received the tenders. We have chosen one of the bidders and we are hoping to have the study ready within the next six or seven months.

Q126 ***Lord Mawson:*** Are the people tendering academics or businesses who run serious databases? Who are these people?
Ms Vassiliadou: The call for tenders was not limited to certain types of field, whether they were academics or businesses, but I can disclose that the bidder that has been chosen comes from the business side. It is a joint venture of companies that already have experience with such processes.

Q127 ***Lord Marlesford:*** Can I follow up that earlier question and your answer to it? Presumably there might be both operational and cost benefits in basing the new system on one that already exists, and the only ones I know of, and perhaps you would fill us in about others, are the United States, Australia, France and the UK. Other things being equal, would you prefer to base it so that it is an easy interface and you do not duplicate?

Ms Verkleij: For the time being we are aware of the US system and the Canadian one, and we are in negotiation with Australia and are trying to understand their system. The difference between the European Union and those countries is that the three all have federal customs which receive the data from inbound and outgoing flights. We do not have federal customs in Europe, so to us there is still a choice to be made between a central database or decentralised databases. In terms of the technology, the US, Canadian and Australian systems are all different, and it never ceases to amaze me how different they all can be. It is a debate which we never really went through in detail because in the negotiations we had with the US and Canada, and also in the current one with Australia, we do not think it is appropriate that we tell them what kind of technology they should choose. That is their choice. We are interested in the purpose for which they want to use the data, the guarantees they want to agree upon and issues like a regular review. Apart from the issue of whether the data should be pulled from a database or be pushed by the air carrier to the law enforcement authorities, we did not really go into very detailed debate on how to build an IT system It is an issue for which we have launched the study in order to get a better picture. It is also an issue for the air carriers, of course, because each time they have to accommodate different systems, so it will become an issue at some point in time. What we try to do is make life for air carriers easier by providing them with the possibility to choose an intermediary. For example, take air carrier A, which already has to send data to, let us say, Canada. In the Canadian case there is already an intermediary which takes up the function of reformatting the data and filtering the data to which Canada should not have access, and they send it in a certain format to the Canadian authorities so that it is easily accessible to the Canadians. The air carrier could use that same provider in order to meet the requirements later on of the European authorities, and that in our view is a way of facilitating and accommodating part of their concerns and also making it less costly. That choice is being provided for in the proposal. Again, that will feed into the debate on the IT system and on a centralised or decentralised database. We try to the greatest extent possible to make the issue as workable and as operational as possible. Of course, we are not IT experts and IT development sometimes goes so fast that if you have identified a certain system it may be outdated in five to 10 years' time, so you have to be very careful, but it will be very much on the agenda at a later stage during the discussions.

Q128 ***Lord Marlesford:*** I was not, of course, suggesting that the EU should tell the countries which have already got systems what IT system to use. I was thinking of building on success, if there is success, in those countries and if there is a common factor. Of course, the other country which I am aware of which certainly has had very early on an extremely effective e-border system, not PNR as such, is Hong Kong. Have you had a look at Hong Kong?
Ms Verkleij: We have heard about Hong Kong and I think also Singapore was mentioned at some point in time as being one of the newcomers.

Q129 ***Lord Marlesford:*** Hong Kong is not a newcomer. They had a system before the British in 1997.
Ms Verkleij: That is very good to know. We will certainly, when talking to the persons who will provide the study to us, raise these issues to make sure that they look at as many systems as possible that are up and running and that provide what they should provide.

Q130 ***Lord Mawson:*** We spent quite a bit of time developing a national IT system, so I am very conscious of the practicalities involved in this, and one very quickly discovered that actually IT is just a tool and behind all that it is ultimately about the relationships between the individual companies and the people who are running a particular aspect of it. That is the key to making it work or not work. I just wonder what you are doing or are going to do to ensure that those sorts of relationships work because that is the thing I would be looking for if I were doing your report.
Ms Verkleij: You are right, and that is why the IT discussions should not be too early in the overall discussion, because you need to find out first about those relationships before you decide on the IT, because the IT is indeed a tool. It is not the solution to the problem in the sense that it provides you with an answer on whether the system should be centralised or decentralised. That is not going to answer those questions. You have to answer the basic questions first before you can design the IT which you think should provide you with the answers to your issues; you are quite right.

Q131 ***Lord Dear:*** Before I get to the point I particularly want to raise, can you clear up a point you have already touched on in terms of definition of terms? As I understand it, there is no set definition of, say, terrorism or what is serious organised crime. Am I right in thinking that?
Ms Verkleij: Yes.

Q132 ***Lord Dear:*** Different countries could have slightly different terminology?

Ms Verkleij: Yes.

Q133 ***Lord Dear:*** And that could lead to whole swathes of criminality and serious offences being included or excluded, depending on how it works?
Ms Verkleij: You have touched upon the central point. In a couple of our instruments we talk about terrorist offences or serious crimes, for example. One of the things we try to aim for is at least to make Member States aware of what I mentioned earlier, this list of serious crimes in the European arrest warrant, because that gives us a very clear picture of what we all understand as serious crimes. When you look at that list it starts with what you would normally refer to as organised crimes—human trafficking, drug trafficking and so on, but often, the Union being what it is, the actual definition of a serious crime is left to the Member States. We have such an example in the Data Retention Directive where telecom data retained for use by law enforcement agencies is related to prosecuting serious crime, "serious crime" defined by each Member State. You are right; we do have instruments, as I said, in the European arrest warrant, where we have a list, but it is not exhaustive and it is not binding, which does not make our lives easier. In particular it does not make life easier, certainly not for law enforcement, when you look at cross-border exchanges of information.

Q134 ***Lord Dear:*** The Council puts an obligation on carriers, as we all know, to send information through. That has been in force for a year and a half by and large. Have you had any assessment at all on the use of API data to combat illegal activity that would substantiate the need for additional data?
Ms Verkleij: As you rightly mention in your question, that instrument is related to what we call API data, and API data are a particular set of data. We normally refer to them as passport data because those are the data that are requested to be collected by air carriers. In addition, there are a number of data about the crew and about the flight but those are data which they normally request not from the passengers but from the airlines. In the directive, as you may recall, the set of data are listed and also the purposes for which they are being requested. The deadline for implementation was 5 September 2006. Not all Member States have implemented the directive and their failing to do so means that we do not have a clear view yet of how the data are being used by Member States and how efficient and useful they are for the purposes for which they are being collected. It is unfortunately too early to say yet how Member States are using these data. Our colleagues who are responsible for this directive are looking into this and are identifying the Member States who are late and who have already been given a warning that they should speed up their domestic procedures.

Q135 ***Baroness Garden of Frognal:*** You have already answered the question on whether all Member States have implemented the directive, and you have said no, they have not done that and you were following that up. Has the Commission taken action against any Member States?
Ms Verkleij: We always take action. The first action we take is when Member States have not notified the national measures to the Commission. As from the date of expiry of the deadline an infringement letter is sent to the Member State reminding them of their obligation under the directive to notify national measures, and that is always a moment in time where Member States tell us either they have forgotten and they promise to send the national measures as soon as possible or that they are in the process of doing it, and some also inform us why they are late and that the proposal is standing before parliament and that a couple of procedures will have to be dealt with before the measures can be adopted. It varies according to the Member State but that is a standard procedure which we always start, I think, one month after the deadline has expired. That is then followed up with the Member State. Depending on what they have told us, if they are pretty well advanced in the proceedings before the national parliament we may not always consider it necessary to go for infringement proceedings but instead encourage the Member State to make sure the national measures are being implemented as quickly as possible. It also allows us to identify with Member States whether there may be common problems. It may well be that there is a particular issue on the table which we have not addressed at an earlier stage and which merits a meeting with Member States to guide them through that process.

Q136 ***Chairman:*** With a month's grace and six months that takes us to today, near enough. How many states have you written infringement letters to and who are they?
Ms Verkleij: I shall have to ask my colleagues but I can provide you with that information.

Q137 ***Chairman:*** Can we have that please?
Ms Verkleij: Yes.

Q138 ***Chairman:*** How many, roughly?
Ms Vassiliadou: The large majority of Member States have already enacted legislation domestically for the collection of data.
Ms Verkleij: Two-thirds?
Ms Vassiliadou: It is more than two-thirds. I think it is only two or three Member States that have not yet enacted legislation but most of the systems are not

operational yet. This is something else. It is the second stage that we are looking into.

Q139 ***Lord Dear:*** Can I change the focus to PNR information? As we all know, that is very much in the frame for air travel, but I wondered if you had any views about its extension to other forms of travel, particularly maritime and rail, and whether, if it were left just with air travel, that would be proportionate and proper.
Ms Verkleij: We have proceeded with an impact assessment which has preceded the proposal, and one of the questions on the table was exactly the scope of the proposal in terms of the different means of transport. We have chosen air deliberately, first of all because we have some experience with that.

Q140 ***Lord Dear:*** Because of the USA?
Ms Verkleij: Exactly, and Canada, but also because the information which we receive on a regular basis and which is concerned with security issues indicates to us that the collection of PNR data is most effective for air transport. We had to make a choice. We have to put forward a proposal for 27 Member States where the vast majority for the time being have no experience at all with this; it is new to them. It is new to the European Union to set up such a system, so we want to be both ambitious and moderate, ambitious by proposing a European system and moderate by limiting it to incoming and outbound flights.

Q141 ***Lord Dear:*** From outside Schengen?
Ms Verkleij: Incoming and outbound flights, not including intra-EU flights or even domestic flights, and that is because we think the case for PNR can be made for those kinds of flights and where we have a real security problem to face. Having said that, it may well be that some Member States identify that they may have a security problem, let us say, with certain maritime links. In particular in the south of Europe you may argue that there is a competition between certain maritime links and air routes in terms of the choice to be made by a customer. That is very likely also because of the short distance between Europe and North Africa.

Q142 ***Lord Dear:*** Morocco to Spain would be an example?
Ms Verkleij: Exactly. You may say it is a choice between taking the boat or taking an aeroplane. If those Member States concerned, one or maybe two or three, think there is a real issue there they can deal with that issue. The proposal would certainly not exclude that and would allow them to implement domestic measures which should take care of security concerns, for example, by asking any maritime operators also to collect this kind of data. For the time being the collection of this kind of data is pretty limited in the maritime sector, which is another reason for us not to go European-wide yet. We can go European-wide with air because the air carriers are already collecting the data, so you feed into current practice but add other purposes for which the data will be used. That is why we have limited ourselves for the time being. That does not exclude at a later stage, if we think there is added value for Europe, taking that further step into maritime and maybe also rail, but it already looks difficult enough to come up with a proposal that will work and be up and running among 27 Member States in the area of air, so we thought it better to limit ourselves to air for the time being.

Q143 ***Lord Dear:*** Would that extend to road travel as well? I do not know whether you get much travel, say, from over the Turkish border into Europe, but, assuming one did, the occasional coach party and certainly lots of trucks use it, logically would one extend it to that as well?
Ms Verkleij: That depends, I would say. One of the issues which is extremely important in this whole debate is, do you have a security issue? If you have, what does it look like, because security issues also shift over time so you have to see if these are security issues which are likely to stay with you for, let us say, the coming 10–15 years so is it worth investing in equipment to collect information? The second issue on the table is which kind of information would allow you to tackle those security issues? PNR is certainly one way which is acknowledged to be extremely useful for the airline industry, and maybe also for maritime. I am not so sure whether it would work for road, one of the issues being that you need to collect the data a bit in advance in order to allow law enforcement some time to analyse it. There are a few other issues, such as the quality of the data, which kind of data, the purpose for which they are needed, do I get them well in advance, can I share them, which all enter into the debate and which at the end of the day then define the choice of the data. PNR are important and they are one of the sets of information which law enforcement should have at its disposal. I would not exclude that maybe for road we could identify information which may give the same results or even better results and are maybe less intrusive on privacy but could still give you the tools for the security you need.

Q144 ***Lord Dear:*** This is not a question but an observation. If I were seeking to penetrate any country in Europe and I knew that there was for me a difficult hurdle to cross using an airline, I would immediately go to maritime or road. I would search for the weak link.

Ms Verkleij: You have a point. That is exactly why when we limited ourselves to air we wanted to cover all the Member States, because it would not look very clever to have a loophole over there. You are right. The fact that we do not also cover maritime, rail and road does pose security issues. On the other hand, you have to take measures step by step. If we were to go for the big bang we might end up with nothing after five or 10 years' discussion because one could imagine that if you went for a huge project, including these modes of transport, it would pose huge challenges in terms of how to organise that, not least because you have to bear in mind also the impact it may have on installing something that looks like border control but is not and how to organise this in a practical way. I think we would probably over-stretch ourselves. Having said that, PNR is one of the means of allowing law enforcement agencies the necessary information to do their job and they are aware of the fact that if you cover a certain mode of transport with one instrument it may lead to people behaving differently.

Q145 ***Lord Dear:*** Displacement?
Ms Verkleij: Exactly, and that is being monitored. For example, it has been monitored that the extension of Schengen has already led to a change in smuggling routes, and that is only one month after the entry into force of the wider Schengen area, so these issues are being observed because law enforcement agencies know it will have an impact. If, for example, our proposal had an impact on the use of the maritime route of transport and Member States thought that that impact was sufficiently important for the European Union to act, we would certainly be looking into that but they have to make a case.

Q146 ***Lord Dear:*** I think I can guess what your answer would be, but I just want to move the focus very slightly onto possibly having the same sorts of controls within Schengen, and even within a Schengen country, not crossing a national border. That is perhaps well into the future but do you have a view about that?
Ms Verkleij: Legally we could do it because we propose is not Schengen related. We are not covering immigration and border control issues. We are looking at data for security issues.

Q147 ***Lord Dear:*** It is a form of control though, is it not? It is a form of surveillance.
Ms Verkleij: Yes, it is a form of control, that is true, but it is not border control. You could argue, legally speaking, that we are not installing border controls, so we would not violate Schengen, and Article 21, I think it is, of the Schengen Convention is not applicable to police activities, but in reality what does it look like? That is the problem we are facing. Again, on paper you could argue with everybody that we are not violating any European rules but if you are being stopped somewhere in France and you have to provide a certain set of data, I think that to you it may feel like you have got a border in the middle of nowhere with the aim of controlling you. That is a very difficult debate. We did not want the proposal to wait for that debate because there is a security issue out there and I think we have to tackle that now and not in five or 10 years' time when maybe we have an answer to that issue. Again, this is also something which is very much linked to Lisbon, as you rightly said earlier. I think Lisbon gives us more possibilities to look into the wider issue of using different sets of data for a number of different purposes and how to fit them in. There are discussions not only on API data and PNR data but also with our US colleagues on what we call the electronic travel application. We have visa discussions. There is a lot going on in these areas.

Q148 ***Lord Marlesford:*** Can I come in on a supplementary to Lord Dear's question? Given that Schengen came in about 10 years ago or plus, if it did not exist, and given today's climate of crime and terrorism and all that, would you introduce it?
Ms Verkleij: I have not given a thought to a non-Schengen area, frankly speaking. Schengen is so much in our minds, in our thinking, and also having to address many difficult questions in the proposal, frankly speaking, we have not given that much thought to it because we have not much time to dig into all the aspects we would have to look at, but giving a thought to it now, I think I only can say maybe. I cannot say more than that.

Q149 ***Chairman:*** I would also like to ask a follow-up to Lord Dear's question, which follows on from our witness this morning whom I referred to. She said, "We have asked the Commission for details of all this. We have asked in particular what is the purpose of this initiative". Perhaps I could put it in a way she might have sympathised with, that here you have a proposal which, as Lord Dear has pointed out, is full of holes; it is like a sieve. If you had a terrorist or a trafficker who made a study of what was going on it would be the simplest thing in the world to circumvent it. You would not use an airline; you would come by car or you would use the train if that were possible. You would not come regularly. You would do it in a cleverly constructed way of avoiding being caught up, and therefore—let me put the question to you—what is the purpose of doing this? It seems to me that anybody with their wits about them can so easily circumvent it and so is it worth the bother and the expense?

Ms Verkleij: Thank you for the question but that to me begs a counter question, and Sophie is not here. That takes as a presumption that PNR solves everything and that is simply not the case. PNR is an additional tool, additional to the API data, to the visa, to other information, the aim of which should be to fit them into a jigsaw puzzle which we then present as tools to law enforcement next to other instruments which should allow law enforcement to look at particular ways of people entering our countries. We have never claimed, and I am sure that Ms in't Veld would agree with that, that our proposal would solve everything. It is aimed to do what it wants to do and that is to give law enforcement information which it does not have at its disposal now for particular modes of transport in addition to already available data. It is meant to strengthen i.e. fill in existing loopholes, not to create loopholes. It would mean in that kind of thinking that Parliament would very much be in favour of asking PNR data for maritime, for rail, for road, for everything, for having controls everywhere. I am not so sure whether that is in the mind of the Parliament but we are happy to discuss that. Again, we are not starting from scratch. We are not in a world where law enforcement has no information at all and the Commission certainly does not come with a proposal and says, "This is the panacea to all your problems", because it is not. It provides a very precise set of information of which is already known that it fills in a gap in intelligence which law enforcement gets by identifying passengers through passports or through the API data so that when you present yourself at the border they know you are indeed the person you tell them you are, and linking that into your flight arrangements and maybe as a result of looking at additional information, so you have a whole set of information out there. The interesting issue of PNR is that it links, let us say, the API data and other data in a way which certainly then gives a clue to law enforcement, but again it is only a part of a much wider set of information. We are not creating loopholes. We are adding information which at the moment is not at the disposal of law enforcement. I do hope that alleviates a little your concerns about creating loopholes.

Chairman: I see what you mean. Lord Dear, have you completed what you wanted to say in this section?

Lord Dear: Yes. I have got this mental picture of plotting an offence against the Belgian state and how I would do it, and I can see a lot of routes available. Thank you very much.

Q150 ***Lord Marlesford:*** Article 3(5) allows data to be used to create risk indicators. To some extent that could be said to involve passenger profiling. Passenger profiling is controversial. To put it very simply, I suppose the argument for it is that with limited resources you focus them on limited law enforcement, and also if you are trying to catch the bad guys you want to do it without hassling the good guys. Against it, of course, there is the suggestion that passenger profiling can create what one might call prejudicial discrimination. First of all, do you agree that the provisions of 3(5) will result in passenger profiling and, secondly, do you have a problem with it?

Ms Verkleij: We have had this discussion to some extent in the LIBE Committee in Parliament with Baroness Ludford, who asked us what the definition of "profiling" was in the European Union, but we do not have one. There is no Commission definition, there is no European definition either of what profiling is. The great advantage of PNR, and our UK colleagues who are responsible for Semaphore, explained that very clearly to us, is that it allows you to move away from looking at somebody at the border and thinking, "He or she may be a threat", and on what basis you define that. They explained to us that in their system each law enforcement authority defines the risk indicators according to the type of crime you are looking at, so each type of crime is based on what you may call certain behaviour, say, paying cash, taking a certain route, travelling together or travelling alone. The more precisely you define these indicators the more targeted you can be because it allows you to feed into the system very refined risk indicators which you then match against PNR and that then allows you to get a view of people. It is true that PNR data to a large extent are behavioural data. You may say that that looks like profiling. For example, a marketing company may look at the way we behave in the sense of do we buy certain products at certain shops at certain times, and how expensive are the shops? That is also a kind of behaviour. You may call that profiling but I do not think that is the issue. The issue to us is, have we identified the right set of data which allows us to identify high risk passengers? These risk indicators, as we call them, being based on intelligence, information, facts, should move you away from looking at the person at the border and saying, "That person looks a bit risky to me". It takes you away at least from profiling not based on underlying factual information, which could be every profile. We ourselves in some instances, travelling through Europe together have been subjected, I would say, to some profiling where at some instances they took a very long look at my colleague and not at all at me, and vice versa, and we said to ourselves, "Both of us could have been equally dangerous". I do not think it gave the guy at the border any clue by just looking at us. That is exactly what we want to avoid, that their decisions are not being taken on the basis of facts which are fed into a system and which help law enforcement and in particular the people at the border to identify the people at whom they should

have a closer look, because that is what it is at the end of the day. It does not identify you as somebody who indeed poses a risk but who may pose a risk, and on the basis of additional information they try to find out what kind of person you are and what intentions you may have. I think the proposal itself excludes using data which are based on religion, race and ethnic origin. The proposal expressly excludes that because we do not think that kind of information serves the purposes of the instrument.

Q151 ***Lord Marlesford:*** But when you implied that it would be a substitute, are you suggesting that experienced immigration officials, not unlike experienced customs officials, who do have a sixth sense and can sometimes identify people should then not be allowed to do this, because it seems to me it would be much more sensible to say that the new system would supplement rather than be a replacement for the way they do it now.
Ms Verkleij: I would say it supplements. The US has given a very nice definition of what PNR is. They call it a "decision support tool", and that is exactly what it is. At first instance it allows you to go through a whole list of passengers and say, "Okay, where are the matches against my risk indicators?", and then the human being comes in and looks at those particular cases with his or her experience, asking for additional information, and if that, on the basis of that information, triggers an alert, as Semaphore calls it, then there is the need to talk to that person and have a closer look. But you are right: the human intervention is there and should always be there and it is even a privacy requirement. It is an issue which serves both law enforcement and privacy because, as you say, of course, the trained officer with a sixth sense will also know which questions to ask and which additional information to look for. Privacy tells us that you never should have a system where a decision is taken purely on the basis of what an IT system tells you. The two meet together and I fully agree with you: it allows you to concentrate better on certain passengers and also to concentrate your resources better on who you think should not enter your country.

Q152 ***Chairman:*** Can you just go a little further? You talk about indicators. How are they arrived at and who defines them?
Ms Verkleij: They are being defined by the law enforcement authorities and they are being defined on the basis of regular reports they get, and the reports are related to the types of crimes that are committed, so they get reports on drug trafficking, on human trafficking and also trafficking in minors. One of the specific features of our proposal is that we have added six additional PNR data elements to the list, which are to focus on minors travelling without either parents or others, because one of the issues which is of growing concern in Europe is trafficking in minors. It is also a particular concern of Vice-President Frattini, who is focusing his policy also on children's rights, so it is very much at the heart of his policy. These risk indicators are being defined on the basis of what intelligence tells these law enforcement authorities, defined according to the kind of serious crime you are looking at. It is also based on past experience, and the PNR feeds also into the system because the PNR tells you at some point in time certain patterns, be they travel patterns or other ways of behaving. It means that the risk indicators do not stay stable over time. They need to be updated on a very regular basis. I recall going through the transcript of your meeting with your Minister, and she gave the example of a certain type of passport which was being looked at during a couple of weeks on entering a particular country because law enforcement had information that quite a few of those passports had been forged, so you see it means that the risk indicators have to be updated on a very regular basis, showing that indeed these are the issues we should look at.

Q153 ***Lord Mawson:*** Do you know whether the profiling of passengers under the Framework Decision would raise constitutional concerns in any Member States?
Ms Vassiliadou: I can say that during the discussions in Council no Member State raised concerns, so we are not aware of and have not been pointed to any such concerns—a short reply.
Chairman: A short reply and very much to the point; thank you.

Q154 ***Lord Mawson:*** The UK believes that sensitive personal data are useful and would like the processing of sensitive personal data to be allowed under the Framework Decision, subject to specific data protection safeguards. What is your current position on that and what do you believe should be the specific safeguards in place?
Ms Verkleij: We have been very strict with our proposal. Again, bearing in mind the different sensitivities of different Member States on these issues, we had quite long discussions when we negotiated with different countries on these issues—how far should we go, what should we allow third countries to receive, and in particular sensitive data were part of that discussion. There are a number of Member States which share the opinion of the UK that it may be worthwhile to be given the possibility to use sensitive data. We for the time being still need to be convinced of that. We are open for discussion, for contemplating whether sensitive data could be useful, but there is a case to be made because sensitive data are a particular set of data within privacy and

you need to argue your case a bit more strongly compared to other types of information. It cannot be entirely excluded but Member States should tell us precisely why they think they need the data, which kind of data they need, for which very specific purpose and what kind of guarantees they have in mind. That is the kind of debate we are open to, but they need to make a case.

Q155 ***Lord Teverson:*** One of the things that came up in our earlier meeting with Sophie in't Veld that seemed to some of us as also important in relation to the American agreement was how on earth, in a parliamentary democracy (or at least in America's democracy), once these systems arrive, you can evaluate them in terms of cost/benefit, in terms of whether the Member State or the Commission are keeping to the rules with regard to data and whether the results of this in relation to decreasing organised crime or terrorism or whatever are happening. How do you do that because as soon as governments and maybe executives like the Commission have got control of this they naturally do not like being accountable to parliaments and in this area they can say, "Sorry, we cannot give you all that detail because it would prejudice national security"? In terms of safeguards, how do we safeguard democracy and parliamentary accountability for this sort of system within Europe?
Ms Verkleij: I tend to disagree with a position which says that governments or the European Commission are not accountable for this sort of thing. It cannot be the case and it is not the case, and we do see that also in national parliaments. You need special provisions for making sensitive information available to Members of Parliament, so you need special procedures, you need special guarantees. When we discussed with the European Parliament, for example, actual cases which are the result of the use of PNR data, this is law enforcement sensitive information. It should not be withheld from them in discussions but we cannot discuss that out in the open because it may reveal certain information which may make it very useful for those out there who try to circumvent the system. It may be that we still need to work on establishing a closer working relationship with the European Parliament but we have already had meetings with the Parliament. In particular I recall one meeting in June 2005 where Ms in't Veld was present when the then acting Under-Secretary of the US, Randy Beardsworth, came over from the US to show a selected group of the LIBE members actual cases dealt with under the US/EU PNR agreement, and he had with him an assistant who showed us the cases. We could not make copies and we could not keep that kind of information but we were allowed to have a look at that information, and we were allowed to have a wider look at that information a couple of months later when we went to the US for the joint review, so there are ways of organising yourself to get a much better picture of how it actually works. There is a working mechanism of oversight in the different agreements but it has its limits. It has its limits because at the end of the day it contains information which is very law enforcement sensitive, but it does not mean that we cannot talk to our parliaments; it does not mean we cannot talk to the European Parliament. The European Parliament, for example, was given a copy of the full report of the 2005 joint review where we described our findings. The findings are the public part; everybody can read our findings, but the information on which the findings are based is classified information because there you will find details on how the US system functions. There is no reason to exclude parliaments from this kind of debate by saying, "This is very sensitive information", but you need to handle it with care and provide certain guarantees.

Q156 ***Lord Teverson:*** Could you identify a best practice worldwide for this at the moment?
Ms Verkleij: I think that would be difficult because we all have our perceptions of what we could and could not say in the public domain. Even within the Union there are differences in terms of how far our transparency regulations should go. It is a bit difficult to identify overall best practice and it may even differ from one kind of information to another. However, I think there is an overall necessity to provide certain guarantees so that there is democratic oversight and also that there is oversight over the programmes in terms of efficiency. This is always a general law enforcement issue because how do you demonstrate the efficiency of your system? How do you demonstrate that because of, for example, a PNR system fewer terrorists are tempted to travel to your country? How do you know? How do you know indeed how many terrorists have any intention to travel to your country? I do find that kind of debate very difficult.

Q157 ***Lord Teverson:*** But you have some of the best brains in the world in the Commission. That is what we pay you to do.
Ms Verkleij: I will certainly pass on that compliment to my colleagues. There is one limitation which we face and that is that we are not in intelligence. That is outside the scope of our activities and that means that there is a certain reluctance also within Member States to give us intelligence, but it is part of how the Union is set up. You do get information but we also ourselves have to ask for information and that is what we provided in the agreements with the US and Canada, oversight mechanisms, and we will also provide one in the Australian agreement so that we

can go over with a team composed of different people with different expertise and see how it works.

Q158 ***Lord Teverson:*** I have forgotten on this particular Framework Decision—is there a mechanism for oversight within this decision at the minute?
Ms Verkleij: Do you mean our own European PNR proposal?

Q159 ***Lord Teverson:*** Yes.
Ms Vassiliadou: Yes. There is a review section where the whole proposal will be reviewed in three years from the deadline for its implementation.
Lord Teverson: I will have to re-read it. I apologise that I have forgotten.

Q160 ***Lord Marlesford:*** You can have a system which appears to operate very well and is quite resource intensive, and then you suddenly find a total gap. If I give you a recent example in the UK, we have a Commissioner for Interception of Communications who checks that the appropriate warrants signed by a secretary of state have been made. That Commissioner is normally, I think, a senior judge and he reports to Parliament and all the rest of it. The other day it was suddenly discovered that a Member of Parliament—it happened to be a Member of Parliament, which is really why it came out—was visiting one of his constituents in prison and his meetings with this prisoner were being bugged and it was found that this was perfectly legal. It was being done by the prison authority at the request of the police but it was perfectly legal and nobody suggested there was anything wrong, but of course it made a total nonsense first of all of the idea of secretaries of state having to give permission for interception of communications and, secondly, having a commissioner to check that it had all been done properly. You may have some difficulty in designing an oversight system which is anything like watertight.
Ms Verkleij: Let us be realistic about this and be ambitious in terms of working towards a functioning oversight. You will discover because of your oversight that there are gaps and there are problems, but that shows again the need for an oversight system.

Q161 ***Lord Teverson:*** Under Article 11, all processing of PNR data will be governed by the Data Protection Framework Decision, something that we have talked about within this sub-committee over the last couple of years. Given that the scope is limited to cross-border data exchanges, do you consider this data protection regime to be adequate? If you get rid of the Third Pillar and we move on to a post-Reform Treaty what happens then?
Ms Verkleij: When we worked on the European PNR proposal the discussions in Council on the Framework Decision and data protection were still ongoing, and it was not clear at that moment in time what the scope of application of the Framework Decision on Data Protection would be. We had hoped that we could come to an agreement that it would be applicable both to domestic and cross-border processing and with that in mind we included a reference to the Data Protection Framework Decision, hoping that it could cover these forms of processing and also because the aim of the Framework Decision is indeed to provide adequate privacy conditions and guarantees for the use of personal data by law enforcement activities, exactly what the PNR proposal is about. It turned out differently. The political agreement reached in Council in November limited the scope of application of the Framework Decision on Data Protection to cross-border and that, of course, has triggered some debate in Council about the application of data protection provisions. At this stage of the debate some Member States have raised this issue and have suggested not simply to have a reference to the Framework Decision on Data Protection but to include specific data protection provisions in the instrument so as to make sure that guarantees similar to the Framework Decision on Data Protection are also applied within the framework of the PNR Framework Decision. That is the strength of thinking for the time being.

Q162 ***Lord Teverson:*** It is an evolving area?
Ms Verkleij: Exactly.

Q163 ***Lord Teverson:*** The Data Protection Framework Decision applies only to data processed by public authorities responsible for law enforcement. What data protection provisions will apply to private sector bodies involved, such as airlines and their intermediaries, for example SITA, and all the multiple agencies that are involved in handling this data at some point?
Ms Verkleij: It is important to bear in mind again the scope of the proposal and its limits. The proposal starts at the moment that data are transferred by air carriers to law enforcement authorities in Member States. The collection of PNR data by air carriers as from the moment that you make a reservation for your trip, at the moment of check-in and the moment of boarding is done for commercial purposes. That means that that kind of processing remains entirely covered by the Data Protection Directive of 1995. There is no change in the data protection regime as far as that is concerned because the directive is meant to cover those issues. What we had to cover was first a change in purpose, so the use of the data by law enforcement means that it is no longer for

commercial purposes but for law enforcement purposes, and that obliges us under our privacy rules to provide for a separate legal basis. It also means that you then have to look into specific data protection provisions which relate to law enforcement, so as from the moment of transferring the data to law enforcement authorities the law enforcement data protection provisions become applicable.

Lord Teverson: I am sure as normal citizens we will all understand that perfectly.

Q164 ***Chairman:*** Thank you very much. The very last question falls to me, which is to ask you how you are getting on with the fresh proposal which you will be presenting once the Treaty of Lisbon is put into effect. Is it nearly complete or have you still got quite a lot of work to do on it?

Ms Verkleij: We are all hoping, of course, that Lisbon will enter into force on 1 January 2009 because that gives us a very concrete timeline to work against. What we aim to do is discuss with Member States as much issues as possible, take stock when Lisbon enters into force and reformulate them in a new Commission proposal. We then have to see whether we have to go through a new impact assessment, whether we have to go again for wide consultation. We will have to see. These issues always trigger a lot of interest, for which we are very grateful, but it also means that you do need a bit of time for a proposal to go through this whole process, which means that the discussions in Council and all the work we have been doing is not lost. On the contrary: as you said earlier, with Lisbon and with the work done in the run-up to Lisbon, we may hopefully get a better result so let us work on that presumption.

Q165 ***Chairman:*** Thank you, both of you, for coming. You have answered our questions with a great deal of charm and a great deal of clarity. Thank you very much. I must say the face of the Commission this afternoon compared with the portrait that was painted of it this morning is somewhat different, but we much appreciate your presence. We are hoping that we shall agree on a report by the end of this month and publish it towards the end of May. We shall be glad to send you a copy of it and no doubt that will help you to prepare the next proposal I referred to next year. Thank you very much indeed.

Ms Verkleij: Thank you. We are looking forward to receiving your report and feeding that into the debate.

Chairman: Good.

WEDNESDAY 2 APRIL 2008

Present	Dear, L.	Marlesford, L.
	Garden of Frognal, B.	Mawson, L.
	Jopling, L. (Chairman)	Teverson, L.

Examination of Witnesses

Witnesses: MR PETER HUSTINX, European Data Protection Supervisor, MR H HIJMANS and MRS A C LACOSTE, EDPS Secretariat, examined.

Q166 ***Chairman:*** Mr Hustinx, welcome and welcome to your colleagues as well. I will ask you in a moment to introduce them for the benefit of the shorthand writer. As you may know, we are on the record. The Committee is doing a brief inquiry into the latest proposal for a PNR system in the European Union. We are hoping that we shall come to an agreed report by the end of this month and publish by the end of May. That is our intention at the moment. We have had evidence in the past from our Minister and we have had evidence this morning from the European Parliament and, as you know, just now from the Commission, and so we are particularly grateful to you for coming to, hopefully, dot all the i's and cross all the t's. Perhaps you would begin by introducing your colleagues.
Mr Hustinx: Left of me are Mrs Lacoste and Mr Hijmans, both Legal Advisers at the EDPS Secretariat.

Q167 ***Chairman:*** You have said in your Opinion that, while the purpose of the draft Framework Decision is clearly limited to preventing and combating terrorism and organised crime, the means used to achieve this purpose "leave room for discussion". Could you tell us what you meant by that?
Mr Hustinx: That latter part was an understatement and the first part was a positive remark that there is no discussion in my mind on, say, combating terrorism and organised crime, although we are used to purposes like this including all other serious crimes and then we end up with a range of purposes. Here we noticed a quite clear focus, but with a purpose only the proposal is not fully satisfactory. We have made this comment in the context of the part which is on legitimacy and there we found quite a lot of unsatisfactory elements. If you analyse the proposal, as you and we have done, the heart of the matter seems to be about collecting as many data about travellers as possible with a view to developing risk assessment. That is an important emphasis, and that is not with a view to combating terrorism, identifying whether this person is on a list and whether this person should fly or not, let alone on a list of wanted terrorists. This is about data concerning all travellers in and out of the EU with a view to risk assessment. The criteria regarding the standards and methods used were unclear and are still unclear, so you will find some reflections on this particular tool. The Opinion says that basically it is a proposal in layers. The purpose is in layers. It is all about this particular tool and it seems to involve a lot of information. All the issues we have raised in that context are about the tool. There is an issue, and maybe we will come to this, as to whether these data may also be used for other purposes, but I have accepted for the time being this particular targeted purpose of combating terrorism and organised crime. What I found worrying was that the evidence to support the need for this particular tool was very scanty; it was anecdotal; it was by reference, and the proposal we looked at—and I want to emphasise that we have analysed the Commission proposal dated 6 November and its related documents, impact assessments and things like that—did not contain a convincing need. The issue of proportionality was dealt with in an unsatisfactory way, so all the usual tests which the case law of the European Court of Human Rights applies to see whether a particular proposal is in line with Article 8 of the European Human Rights Convention were quite unsatisfactory in relation to the purpose specification. Once you go beyond the mere statement that this is for combating terrorism and organised crime, the relation between the means and the purpose, the safeguards and the precise descriptions, is a citizen able to predict what will happen to his data? Not at all at this stage, and so we say leave room for discussion. The Opinion is making that point very clearly.

Q168 ***Baroness Garden of Frognal:*** What objections do you see to Member States making use of PNR for wider law enforcement and for immigration purposes and what would the data protection implications of that extension be?
Mr Hustinx: That is an important issue and I see problems if the answers are not satisfactory. It is an important issue because the purpose specification is the key element in making a particular proposal legitimate under the human rights standards, but is also the pivotal element of any data protection arrangement if you want to make the safeguards appropriate. Therefore, if collection of data for a

certain purpose is acceptable, it is a separate issue whether these data are then used for other purposes and, if so, whether these purposes are compatible and, if they are incompatible with the original purpose, whether an additional test is fulfilled, a test which is in data protection law and which is an international test, and it is a separate step in the analysis. Let me approach this from the other end: we have the data so we might as well use them and why should we not use them if it is efficient? That is not the kind of thinking which I subscribe to. I can imagine a case for that being made and then my answer would be that under these circumstances we should be paying attention to the criteria under which this kind of efficiency is acceptable under the existing human rights standards, and all that was not in the proposal. In fact, the Commission did not open the box for use for other purposes, although I know the Council is discussing some of this. Under the existing rules (all members of the Council agreeing before there is a decision and in the future a majority agreeing before there is a decision) "used for other purposes" is problematic if it does not fulfil all the requirements. This is all the more relevant if the purpose analysis is part of an invasive technique. If you accept something on, say, an anti-terrorism pretext, the result of these invasions should then not be used lightly for other purposes because we did not lift the bar to that level to make it easy for all other purposes. This is the kind of thinking, not to make it difficult for law enforcement; that is not my intention, but we have been applying the tests to see whether this proposal met the standards which the Commission subscribes to in its official policy and its impact assessments, and this is what the Opinion is doing.

Q169 ***Baroness Garden of Frognal:*** Could I draw you specifically on the letter from the UK Home Office Minister to Vice-President Frattini where she argues the case that Project Semaphore actually produced results and therefore it was a useful use of PNR for other purposes? Does that in any way influence your argument?

Mr Hustinx: With your permission, my Lord Chairman, I think we are at a point in the discussion where I have to make you aware of some of the limits. First, I do not have the letter; it has not been sent to us, although if it is an interesting letter I would love to read it.

Q170 ***Chairman:*** Do you want to adjourn for two minutes to read it?

Mr Hustinx: No. I think I can comment without reading the letter. Maybe that is even better. I can imagine a stakeholder of PNR arrangements (and it is your responsibility to see whether you find them appropriate) writing a letter with flying colours to convince not only the Commission but all other governments represented in Council, so I would rather be struck by a lack of evidence than by the glowing language being used in it. If I were to analyse that, I would say how precise is the language, so maybe you should ask how precise is the language? Is it, "We find it very useful"? We are struck by one element, a lack of precision when it comes to combating terrorism and how effective this means is in terms of terrorism, and this applies to the US experience and the Secretary of Homeland Security has been speaking on this in the European Parliament. He was careful to annex a list of some 20 or so examples to his speech and it was all about drugs and people evading paying taxes and things like that, but there was very little in terms of precision on terrorism. Maybe that is not possible in this area but, of course, it complicates matters if you want to build a focused tool and measure whether this is legitimate, so I am afraid we are left with exactly this point. We have the Advance Passenger Information system. That is identification information, basically, but the key issue is whether the additional invasion from a wide-scale PNR system is appropriate and necessary. I think Member States represented in Council will also find that puzzling, some more than others, and there is an ongoing discussion on this. I think that is appropriate and it should proceed, but so far I have not been presented with convincing evidence that such a system is necessary, and if we look, for instance, at the report of the US GAO, the research bureau of Congress, that also raises issues which we find quite worrying.

Q171 ***Chairman:*** Can I try and sum that up by asking you whether, in terms of your current attitude about this proposal being unsatisfactory and unclear, this is typical of proposals put up by the Commission or the Council, that after its first form as an embryo, if you put it that way, as it goes through its development and discussion it becomes less unsatisfactory and more clear? Is this a typical situation with a new proposal as far as you are concerned?

Mr Hustinx: No, I do not think it is typical, but it happens and it might have happened in this case. It may happen in this case. It is not typical because we are at the stage when a proposal is sent for official comment. We get proposals for informal comment and that is part of the thinking process. Some are more convincing than others, but this proposal, which was exceptional and very atypical, generated my first Opinion which was plain negative. The others have been critical but this was very negative. The language was *non sic*, not in this way. The legitimacy is, in the end, with some room for discretion, a political question in the purest sense of the word. This is why the Opinion moves beyond that point and says, "If you think all these questions have

been answered satisfactorily, you should provide verifications on applicable law, more precision and more safeguards". I can imagine a scenario where, if the Council were convinced on the first issue, progress could be reached by adding more specificity to the proposal, but under current rules that happens by unanimity; otherwise there is no decision. This is difficult to predict but my sense is that this will take more time. This is a proposal which eventually needs to pass the test to convince both Council and Parliament, and from my point of view I welcome that because usually co-decision, with all the consequences, is a safeguard for better decision-making with Parliament as a strong stakeholder of fundamental rights protection, but the Committee of Civil Liberties, Justice and Home Affairs is also very much aware of the need for law enforcement. This is just a hypothesis and it may well be that in the course of time things will go better, but I still find it worrying that we have not heard a convincing story yet about why it is so useful.

Q172 ***Chairman:*** What efforts have been made by the various parties of the Commission and the Council to enter into discussions with you to try and clarify the situation and, bearing in mind that this issue looks as though it is going to go to co-decision, have you started having discussions with the Parliament about it?
Mr Hustinx: It is normal that EDPS opinions are presented in Parliament. I take part in discussions in the LIBE Committee. This Opinion will not be an exception, I think. The Parliament will have a hearing soon, so that process is ongoing. As for the Council, I had the pleasure to be able to present this Opinion last week to the working party in charge, and we then also observed part of the following discussions in a more limited group where the evidence and the experience were being shared, and up to now the information we have is that discussion is taking place. My impression is that some scope for improvement is being used, particularly by adding safeguards, but the convincing case for necessity and proportionality has not been made.

Q173 ***Lord Dear:*** I have a couple of questions which I am quite sure you will answer very quickly and that is fine, but if I may I would like to continue this current theme because I confess to being confused. Let me explain why. There is a body of thought that says the more information you can get in the better, from airlines, from wherever. We can put it all into a database and we will therefore have available what the normal traveller looks like, what their patterns look like, and we will then feed against that the profiles of individuals travelling on this particular day. Most of them will fit the average but some will not and it is the ones that do not that we will be interested in. I am over-simplifying it but you take the point. Is there objection in data collection terms to that approach, because it is predicated on getting all the information? That is the weak link, I think, in the argument.
Mr Hustinx: That is indeed a problem to start with. Getting as much information as possible is the worrying thing.

Q174 ***Lord Dear:*** From commercial sources or wherever?
Mr Hustinx: In this case from a source where the data is collected to move a person from A to B and sending this to another infrastructure which is then doing things which are not clear. That is the worrying thing. To be very precise, if you have a credit card, credit card companies use these techniques to see what your usual behaviour is, and if a credit card is used in Prague and then in Bucharest for money you never spent you can imagine that that is a signal that it may be stolen, so there is some merit to this, and we are not naïve. But this story has not been told and has not been explained, and so far we have not had the kind of evidence which you would expect.

Q175 ***Lord Dear:*** So it turns on transparency?
Mr Hustinx: What I find worrying after a number of years—this is not just fantasy; it is happening in some place in the world—is that we still get signals like, "This is terribly useful for crime. It is very good to catch drug dealers", but that was not what we started to do, although it may be part of organised crime. The focus here was on terrorism. If you have a focus on terrorism, under present rules and discussions that means a certain scope of powers and exceptional arrangements, and this is what I find worrying.

Q176 ***Lord Dear:*** I am grateful to you; thank you. There two specific questions. The first one is about PNR information being collected from aeroplanes at the moment, and the suggestion that you could extend that to maritime and road and rail, particularly maritime and rail. Do you have any problems with that about proportionality, forgetting how difficult it might be, just on the proportionality side?
Mr Hustinx: Your question is, of course, legitimate, but this is my second flag-waving in the conversation because that was not part of the proposal we analysed. If your question is, were we worried that the maritime connections were not part of this, the answer is no. If only because of the sheer size of this project, it would be wise to do this step, and maybe there is a limit to what you can expect in practice, but it still involves all airline connections in and out of the EU, so it does raise a number of issues. I do not think that the issues we have just discussed are affected by it, not including the maritime connections and rail

connections, if they exist, and we might perhaps also then discuss airline traffic within the EU. They are separate issues and they are raised, particularly the second one, as separate concerns.

Q177 ***Lord Dear:*** I was going to ask you about that because that was going to be my second point, which flows on very logically. Forgetting the external border, what about movement within the EU and perhaps within individual countries within the EU?
Mr Hustinx: What individual countries do is, of course, up to them to a large extent, but if this were to impact on the freedom to travel freely within the EU, as it seems to do, then it raises a number of issues—the principle of free movement, but also the Schengen arrangement, so should it be allowed because it seems to be problematic? If the case were made that this is necessary I think it would most certainly mean changing the existing arrangements. More Member States have recently joined the area of free movement. It would be new and I think it would be problematic, and issues of proportionality and so forth would certainly arise because that is also a principle of European law in general.

Q178 ***Lord Marlesford:*** I think we are back to profiling. First of all, is your position that you are opposed to profiling unless there is a good reason for it or are you more widely opposed to it anyway? If the objective of this whole system is to catch the bad guys without hassling too much the good guys, and also given that you have limited resources to focus them where you are most likely to catch the fish, do you accept that profiling is in practice necessary? My other supplementary is that the Commission explained to us how they have taken some care to avoid certain sorts of profiling. The good immigration officer, rather like the good customs officer, will use what one could call the observation and sixth sense way of profiling.
Mr Hustinx: His nose, or whatever.

Q179 ***Lord Marlesford:*** Absolutely. In other words, exactly the sort of profiling which the Commission in this scheme is seeking to avoid using for being worried about it being described as prejudicial discrimination. Do you see this system as being a substitute for or a complement to the existing methods of frontier control?
Mr Hustinx: The concept of profiling is at the same time fuzzy and worrying in some contexts and not in others, and that makes it another problematic thing. You have perhaps noticed that we have avoided discussion about profiling. There are references to two definitions of profiling, some emphasising more the techniques used—data warehousing, computer analysis, and the other more on substance—categorising, standardising, and it is probably a combination of the two and the European Parliament is currently thinking about how profiling could and could not be acceptable. Some of it is mild and it has been around for a long time. I think in marketing, if you want to sell or not sell, you make an offer and it depends what kind of targeting you do and whether it is inclusive or exclusive and what the consequences are. Here we are dealing with an area which is both wide-scale, it involves everybody, and in the context of combating terrorism and not allowing people entry into the European Union or on an aeroplane it has rather a big impact. What is profiling doing here? It is using data from various sources about other people who are associated with you and you fit in the presumption that this may be a risk group. There things start to have quite an impact with the lack of clarity about what a mechanism is. Is this something to correct easily? Well, if you are on the spot and you have to explain that you may fit the profile but there is no reason to be suspicious, it is very difficult with all the powers of government, and so this is an area where you have to be very careful. This is not marketing. This is not red-lining, which happens and which is also quite discriminatory in terms of whether you live in an area where you can get the mortgage paid or not. This is about freedom to move. It is also very close to the presumption of innocence, so in ways which you cannot perceive, understand or predict, you can find yourself in the situation of fitting the profile and there is little defence against it, so the mechanism in this context is I would say inherently suspect. Do I exclude this under all circumstances? No, but it means that using these mechanisms in these contexts on such a large scale requires a very high degree of robust evidence, and there we come back to square one: very little evidence has been produced so far, so this kind of profiling we say is risk assessment and we have been looking in the proposal for mechanisms to detail this. Who is to set the criteria? Who is to set the procedures? The answer is open. I also realise that the proposal is for harmonisation of these practices in all EU Member States and it involves exchange of data, no matter how the practices from country to country will be connected, so you may also feel the consequences of the kind of risk assessment happening in another country, and since people travel they are affected by this as well. The lack of harmonisation of risk assessment practices may therefore affect the freedom to move, to be not suspected of things if you are totally innocent, so maybe also the effectiveness of the mechanism to catch the group you want to catch or identify or eliminate is not terribly convincing for the time being.

Q180 ***Lord Marlesford:*** What about the question about being a complement to or substitute for the existing methods of profiling, the on-the-spot experience of immigration officials?

Mr Hustinx: I would be interested in a comparison of how effective these mechanisms are, say, on a comparative scale. The sixth sense or the seventh sense would be plainly discriminatory, let us say, if you catch people with this religion or this ethnicity, and then it would not be acceptable.

Q181 ***Lord Marlesford:*** It would not be acceptable?
Mr Hustinx: No, of course not.

Q182 ***Lord Marlesford:*** Even if it catches people?
Mr Hustinx: That is a good point. Profiling on the basis of religion and race was not part of the Commission proposal. I think they carefully left it out, so we have no reason to criticise the proposal for that, but I would not be supportive of bringing it in.

Q183 ***Lord Marlesford:*** No, but it is in use, I imagine, on the spot.
Mr Hustinx: Yes. Again, the point is, if the nose of the customs officer is just a disguise for his discriminatory behaviour, I do not think I would be very positive about it.

Q184 ***Lord Mawson:*** I would like you to help me get a handle on it. Who funds you? How do you fit into the scene? How does all that work?
Mr Hustinx: EDPS is not an NGO. It is a European institution, briefly put, so my budget is on the European Union's budget. It is Chapter 8B, if my memory serves me right, 8A being the Ombudsman, and we share the same chapter.

Q185 ***Lord Mawson:*** Thank you. Do you know whether the profiling of passengers under the Framework Decision would raise constitutional concerns in any Member State?
Mr Hustinx: I would think so, yes. It is difficult to make a fully-fledged analysis but, for instance, if you analyse the recent decisions of the German Constitutional Court and the precision with which they look at systematic tracking of licence plates of cars, for example, which was one of the decisions that was then found partly unconstitutional, there is a provisional decision on traffic data retention. My sense is that there is a problem in Germany. Certainly the approach of getting as many data as possible just to do an analysis (the German equivalent of this was found problematic and practised and then criticised in the seventies) without standards being published and accessible I think it is problematic. In the light of the discussion about standards the problem is that it is a categorical judgment which is then applied to individuals with a shifting of the balance of proof and the presumption of evidence. It is close to all this. I think that is problematic and it is bound to be problematic also in the light of the case law in Strasbourg.

Q186 ***Lord Dear:*** It would be problematic, I would suggest, if that presumption then says, "You do not fit the norm; you fit the norm of a terrorist;", or a drug trafficker or whatever, "therefore you must stand trial for that", but if it leads to a train of thought that says, "We have to dig deeper, we have to ask more questions, because there might be something here", is that the same argument?
Mr Hustinx: I see the subtle distinction but this procedural consequence—

Q187 ***Lord Dear:*** Of questioning?
Mr Hustinx: Yes— has practical consequences and some of them may be rather drastic. It may lead to a decision that someone may be an unwanted visitor and is sent back, period, and then it is not tried because that requires more evidence.

Q188 ***Lord Dear:*** That I follow.
Mr Hustinx: We have this fishy feeling and we cannot eliminate this, but how do we draw the line? What are the risks at stake? It does not mean, if someone is issued with a decision of being an unwanted alien and then for the EU that is the immediate consequence, that anything has been proved. It is also difficult to challenge such a decision on the basis of this fishy feeling. That is the problem.

Q189 ***Lord Mawson:*** The UK believes that sensitive personal data are useful and would like the processing of sensitive personal data to be allowed under the Framework Decision, subject to specific data protection safeguards. What is your view on this?
Mr Hustinx: No, my answer is negative. It was not part of the proposal, it is not part of the proposal made by the Commission. We did not find it. In fact, we welcomed it. I think it was not there. In the negotiations with the US there has been a lot of attention given to eliminating sensitive data and that is still part of the agreement, so I do not see it as useful and appropriate to bring it in in this context. In fact, the way it is a eliminated is a bit troublesome but there is no disagreement in the EU/US PNR agreement that sensitive data should be eliminated so, applying that standard, I do not think it is a priority.

Q190 ***Chairman:*** Not at any level?
Mr Hustinx: No.

Q191 ***Lord Teverson:*** Under Article 11 all processing of PNR data will be governed by the Data Protection Framework Decision. Given that the scope of that is limited to cross-border data exchanges, do you consider this data protection regime to be adequate?
Mr Hustinx: No. Maybe you want to have some more explanation.

Q192 ***Lord Teverson:*** Yes, please.
Mr Hustinx: We chose to focus on this issue as one of the four main subjects in the Opinion, and I have been dealing with the Framework Decision in another context—

Q193 ***Lord Teverson:*** As we have.
Mr Hustinx:— so I can refer to that, but this was an occasion to illustrate how unfortunate the limited scope of the Framework Decision is. Apart from the limited scope in law enforcement this is also an area in which you see perhaps public/private co-operation. We see data moving from the private sector to the public sector in a way which is not entirely clear but seems to involve service companies and certain collecting points and transfer points. If you analyse the architecture which the proposal suggests it involves the First Pillar Framework, it involves the Third Pillar Framework, but it also shows gaps between the First and the Third and most certainly also it shows that the scope of the data protection in the Third Pillar is limited. How do you tackle this? The language in the proposal is declaratory, that the standards "shall" apply. You could say they do not, but if the intention is that we want them to apply then it would certainly need upgrading in this context, adding and specifying a number of safeguards and compensating for the lack of scope in the Framework Decision and the lack of protection between the First and the Third Pillars as we see it. It certainly is totally unclear where the one ends and the other begins, and that is an independent source of concern.

Q194 ***Baroness Garden of Frognal:*** In your Opinion you question the applicability of the DPFD to private sector bodies, such as airlines and their intermediaries, and other First Pillar actors, such as immigration authorities, involved in PNR collection and processing. What data protection regime should apply to them?
Mr Hustinx: That is to a large extent the existing First Pillar Data Protection Framework. That is general. It is the Framework Directive as it is being implemented in national data protection law. On a national level quite often it has been implemented horizontally, so including other areas, but it has been a long-term vision that the First and Third Pillars should have a seamless approach. This is likely to happen eventually in the context of the Lisbon Treaty but presently we think that if the EU PNR proposal proceeds it should specify a number of things which apply under the First Pillar, it should add a number of things which do not apply yet and specify in terms of making it fit the subject, and most certainly also the Third Pillar, but we have mentioned that. The lack of precision in terms of which actors have access to data makes it difficult now to imagine what the safeguards precisely should be, but knowing what we know from the airline industry, because we cover some other subjects there, it is likely to involve some of the service companies. The question is, what is their responsibility? That has enormous consequences. Who is acting if an airline shares data with government? That is not so clear. What is the scope of their responsibility? Who should be responsible if something goes wrong? All these issues are important, and then what is the status of a passenger information unit? The proposal leaves Member States some discretion. It could be the police, it could be government, but it could be another body. If it is the police it is likely to be a Third Pillar discussion, but the Third Pillar framework only applies when data move from country to country and at the collection point it does not apply yet. If a passenger information unit is a government agency it is the First Pillar, perhaps; it depends on the task, and this is just a consequence of the current definitions in the Third Pillar Framework. If it is a private body, what then? It is not so clear, but what protection should apply to them? A consistent set of safeguards should apply, for which I take the First Pillar Framework as the measuring stick for the time being, focusing on the risks which arise in this particular context.

Q195 ***Lord Teverson:*** I think probably you have answered this already, but is it feasible to have different regimes of data protection at different stages of PNR processing and the different people involved?
Mr Hustinx: I think it is very complex. At the same time I am aware of the fact that this is a proposal to harmonise national rules; this is not a standards approach, but if this is to work in a legitimate, appropriate and efficient manner we have to mind the connecting points, country-to-country differences, and we have already mentioned some of this. If there is too much scope for diversity within the proposal we will probably see the unfortunate effects of that diversity and they will be to the detriment of the legal protections for citizens but they will also be to the detriment of the efficiency and effectiveness of the system itself. If data come from other countries and if it is not clear what the risk assessment has been in another country then the question is, what does this signal mean? If you start exchanging signals, the quality of which is doubtful, it is bound to raise further problems. I find this lack of precision worrying from different perspectives, including the effectiveness of the system.

Q196 ***Lord Teverson:*** Following on from that and your earlier comments, do you find that both the Commission and the Council really find data protection and your office a nuisance but they have to have it there to apply the democratic brand?

Mr Hustinx: I do not think anyone would subscribe to that language. The proposal is dealing with a very difficult subject. Quite frankly, I think it was premature and there was a reference to this, that it might have benefited from some further thinking. The data protection is part of the set of safeguards which has recently been confirmed in the EU Charter made binding on the Member States and all institutions and bodies in the Lisbon Treaty. It is not easy to implement but I get quite a few letters from commissioners thanking us for the service we give them.

Q197 ***Lord Teverson:*** It is nice to hear that.
Mr Hustinx: Maybe Mr Frattini will write one on this subject as well. If he sees your report he might also think it is helpful.

Q198 ***Lord Marlesford:*** Just following up that theme, in your opinion, if this European PNR scheme comes into force, would a person detained at the border on the basis of risk assessment who is then found not to have been justified in being detained have a case under the European human rights legislation?
Mr Hustinx: I would think so.

Q199 ***Lord Marlesford:*** They would?
Mr Hustinx: Oh, yes, I would think so. But, of course, this is exactly the practical consequence which we have imagined—what could go wrong and what could someone suffering that result do to challenge that? I am afraid that is a difficult course, but if the proposal is made sound, if it is implemented well, then most certainly in the real world things like that will happen, so if eventually it were not be possible to challenge the negative consequences of a legitimate proposal that in itself would also be a source of some difficulty, but I would be very surprised if this would not under all circumstances lead to cases in the court. The criticism I have been making in the Opinion is about the kinds of things which the court in Strasbourg would most likely also feel because that is the standard we have been using.

Q200 ***Lord Marlesford:*** But would the court then be able to require the EU to change the criteria for risk assessment?
Mr Hustinx: In essence, yes, but the story is, of course, a bit more complicated. It would be a case involving a Member State and the Member State is implementing European rules. In future under the Lisbon Treaty the EU will be party to the Convention so the story is a bit more complicated. Again, the German Constitutional Court has in some cases found EU instruments lacking. The arrest warrant was an example, and it happens that international documents under various human rights perspectives are lacking in quality, so it may happen and it will then involve in such a case perhaps a revision of the other rules. That is a scenario that if it is good enough for a majority in Council and Parliament then it could still be subject to such importance. Now we are looking into the future, if the decision of the court affected the European Framework Decision. It could be an issue at the national level as well and that would involve only a change of the law in that particular Member State. All that is possible. The impact this proposal is likely to have makes it, I would predict, quite probable that this will happen sooner or later, that there will be a case in Strasbourg testing these e-border kinds of policies, because that is what they are. So far, remarkably, we have not had cases dealing with PNR, but if this is to proceed on the scale that has been planned then at that stage I expect that will be the test of whether it is an appropriate scheme or not.

Q201 ***Chairman:*** I wonder whether you have consulted the Information Commissioner's Office on the data protection aspects of the United Kingdom's e-Borders project, and what lessons do you think can be learned from the UK project with regard to the wider European Union PNR project?
Mr Hustinx: We have good relations with the Information Commissioner's Office and the Information Commissioner personally. This was not the subject of consultation but quite recently we have been in touch with them and our impression is that there have been some contacts but they were not of the kind from which we could draw any conclusions. It was just satisfactory to know that they were involved but I do not have any detailed information on their input. There is not a document we are aware of on their website and so forth, so it is quite informal.
Chairman: I wonder if any of my colleagues have any further or final questions or points to put.

Q202 ***Lord Dear:*** If we have time I would like to ask one question. You will have to help me with this because I remain a little confused. We all agree, I think, that we should focus on terrorism and serious and organised crime only and not drift down into the lower reaches. We have made that point and others have made it to us. I think we also all agree that the people in that band are in business to make life difficult for the enforcing authorities, in other words, they do not want to draw attention to themselves. If I understand your position correctly, you are very unhappy about the use of data and data profiling in the way in which it is being suggested, and I respect that view. You are also not at all happy with the use of what you call "nose" or hunch or gut feeling.

Mr Hustinx: Yes.

Q203 ***Lord Dear:*** If you exclude nose and hunch because it can lead to prejudice and you do not want data profiling, have you any advice that you would give as to how one protects one's borders?
Mr Hustinx: I have dealt with cases in which you have to compromise some of the principles and compensate for them by other measures, and if you have to accept more collection then you can compensate it by more selection and shorter retention and so on, and there are different ways to do this, but it all starts with clear information on what it is we were talking about. We have not had access to the evidence. It has not been mentioned by the Commission, so I have to fantasise, make it up, and that is very difficult. I can imagine the criteria but it is difficult to do it here, and it would certainly require clear recourse, et cetera, and short deadlines, and that is another point of criticism—13 years.

Q204 ***Chairman:*** I wonder if I could put a final question, which stems from the very first answer you gave to me when I asked you about that phrase, "leave room for discussion". You said you thought that was—
Mr Hustinx: An understatement.

Q205 ***Chairman:—*** very much of an understatement. This whole project—do you think it is a runner? You have pulled it to pieces pretty effectively for reasons I am not going to argue with, but do you think it can proceed?
Mr Hustinx: Maybe not.

Q206 ***Chairman:*** You have put in your Opinion right at the end that provided you can square the thing with Article 8 of the Charter of Fundamental Rights of the Union and various matters are looked at it might go, but it seems to me that one of the messages you are quietly putting to us is that the whole thing is dead in the water. Is that a wrong conclusion or a right conclusion?
Mr Hustinx: It may be true at the end. Let me explain. There is also another scenario and I will try to explain that as well. Putting this very clearly in the Opinion and showing the deficiencies of the proposal helps Council and Member States' delegations and Members of Parliament in their analysis and in some cases it also helps to develop improvements, and if the evidence is presented and it is convincing and Council and Parliament decide in the end to accept this with sufficient precision, safeguards, et cetera, all the clarification needed, I think my Opinion and other criticism will have had an effect. That is one scenario. The other is that I know that thinking about e-borders is not just something of an incident, and there is a tendency about this, but there has been a great increase and a speeding up of everything after 9/11, and some of the things which have happened since 9/11 are starting to produce second thoughts around the world, in the US and other countries, second thoughts, re-thinks, "Haven't we gone too far?". If this is an example of things which need to be re-thought maybe we should do so. If e-borders is so important, and I am referring to this generically although I know it is also the UK term, maybe we should be more careful in putting this together and bring in the detail and the safeguards to make it happen. What we found worrying (another worry) was that this proposal was in early November, but in February already Vice-President Frattini published his vision for the period up to 2015 and it seemed to involve more of this, bigger, larger, and again these documents about the border strategy, the border package, involved a lot of ICT, a lot of monitoring and a lot of analysis, but we have not found the way forward yet, and there is a risk of overdrive with these things so let us slow it down. It is serious business so we should do it seriously and slow down and avoid overdrive and easy conclusions and anecdotal evidence. Is this really what we want? Is it manageable? That is not the first but a very important question. If it is not manageable, if we do not know what the risk assessment is, how are we going to do it right? There are so many questions.

Q207 ***Lord Mawson:*** That sounds fine in a really balanced world until the next serious terrorist incident when to our politicians the general public will say, "What are you doing about it?".
Mr Hustinx: That is exactly my worry and we are here in a reflective mood, I think, but this is not the kind of proposal you do because, by God, you need to do something. That reason was not mentioned. Some things have been done because you need to do something, but now we are starting to realise that not only does everything need to be legitimate for its own sake but the combined effect of all these measures has started to produce an environment we do not want to be in perhaps, and we certainly do not want to extrapolate in automatic shift.

Q208 ***Lord Marlesford:*** Forgive me for being ignorant, but does your position give you any *locus* to comment on national schemes?
Mr Hustinx: I have not been doing this today.

Q209 ***Lord Marlesford:*** No, but does it?
Mr Hustinx: No. My competence is to supervise compliance at a European level and I advise on proposals for legislation. Some of this, of course, has

an impact at a national level. I have been pleased by invitations from your side and similar invitations have come from other Member States and I do not shy away from them, but I am very careful not to comment on national measures and I hope my comments are helpful for you, nevertheless.

Q210 ***Lord Marlesford:*** The reason I was asking you was because, of course, for a lot of the things we have been discussing in relation to the EU scheme the same questions could be asked in relation to the UK e-Borders scheme.

Mr Hustinx: I imagine that is the case.

Q211 ***Chairman:*** Thank you very much. You have answered all our questions and you have put a whole lot of question marks into our minds. Thank you for coming and thank you to your colleagues also for coming. I am sorry they have not had a chance to make a contribution.
Mr Hijmans: Next time we will.
Mr Hustinx: I can tell you a lot of moral and other support was put into this document.
Chairman: It is very kind of you to spend the time with us and we shall find it very valuable. Thank you very much.

Written Evidence

Memorandum by the Information Commissioner

1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000. He is independent from government and promotes access to official information and the protection of personal information. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The comments in this evidence are primarily from the data protection perspective.

2. The Information Commissioner has been examining issues around the use and disclosure of Passenger Name Record (PNR) information for a number of years now, through the mechanism of the Article 29 Data Protection Working Party (A29 Working Party), which is an independent European advisory body on data protection and privacy, set up under Article 29 of European Directive 95/46/EC. The A29 Working Party has produced a number of opinions on the use and disclosure of PNR data and the Commissioner is represented on the A29 Working Party's PNR subgroup.

3. In December 2007, the A29 Working Party produced a joint opinion with the Data Protection Working Party on Police and Criminal Justice (of which the Commissioner is also a member) on the Framework Decision on PNR. The opinion stresses that the EU data protection authorities have always supported the fight against international terrorism and organised crime. Further, they recognise that some use and disclosure of PNR information might be valuable for these purposes. However, any limitations of fundamental rights and freedoms have to be well justified and has to strike the right balance between demands for the protection of public security and the restriction of privacy rights. The opinion concluded that the following data protection concerns were raised by the Framework Decision on PNR.

- The proposal does not justify a pressing need for the collection of data other than Advanced Passenger Information data (which is basically the information on the machine readable zone on a passport).
- The amount of personal data to be transferred by air carriers is excessive.
- The filtering of sensitive data should be done by the data controller.
- The "push" method should apply to all air carriers.
- The data retention period is disproportionate.
- The data protection regime is completely unsatisfactory: the rights of the data subjects and the obligations of the controllers are not specified anywhere within the Framework Decision.
- The great deal of discretion left to Member States might result in varying interpretations of the Framework Decision.
- The data protection regime of onward transfers to third countries is unclear.

4. The Commissioner strongly supports the findings of the A29 Working Party opinion. A copy of the opinion can be viewed at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp145_en.pdf.

5. As the Committee may be aware, the UK Immigration, Asylum and Nationality Act 2006 (IANA) confers far-reaching powers on various border control agencies to collect, use and share information. However, the provisions of IANA appear to go further than those envisaged under the Framework Decision on PNR in that:

- the purposes for which information can be shared includes wider police purposes, immigration purposes and for any Revenue and Customs purposes;
- IANA provides for a Code of Practice, which interprets these purposes very widely, including broad, poorly defined purposes such as "protecting the vulnerable";
- the broader IANA purposes may mean that the single point of entry for PNR information, which has already been set up by the UK Border and Immigration Authority, may not be compatible with the single point of entry envisaged for narrower purposes under the Framework Decision on PNR;

— the provisions of the Framework Decision are limited to PNR information from air carriers, while IANA includes all passenger, crew and freight information from air, sea and rail carriers; and

— under the Framework Decision, a list of 19 data elements are provided to the relevant authorities, whereas under IANA all of the data sets held by the carrier must be provided to the relevant authorities.

6. The Commissioner is happy to provide any further information the Committee may require.

Richard Thomas
Information Commissioner

19 March 2008

Printed in the United Kingdom by The Stationery Office Limited
6/2008 396478 19585